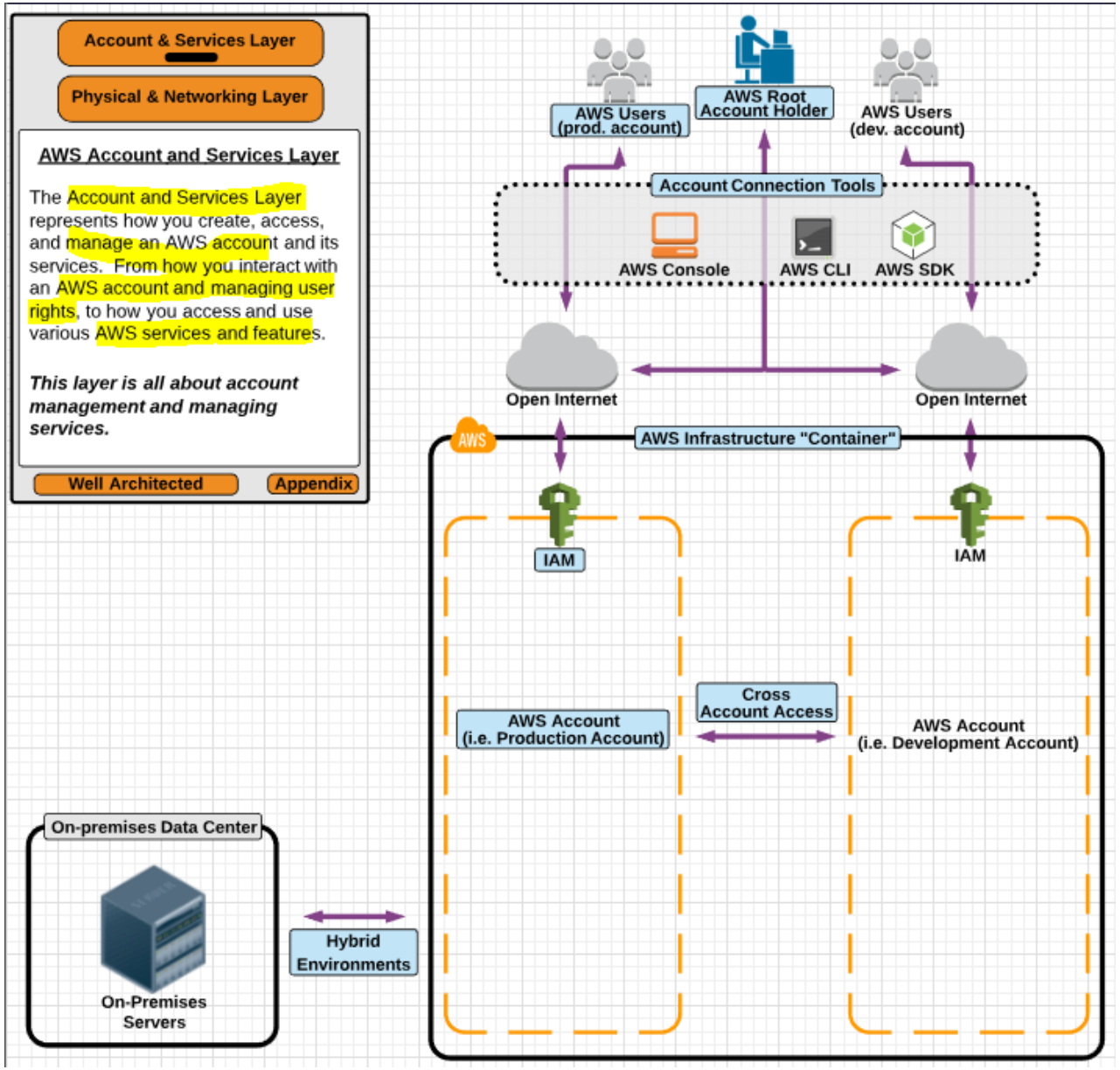
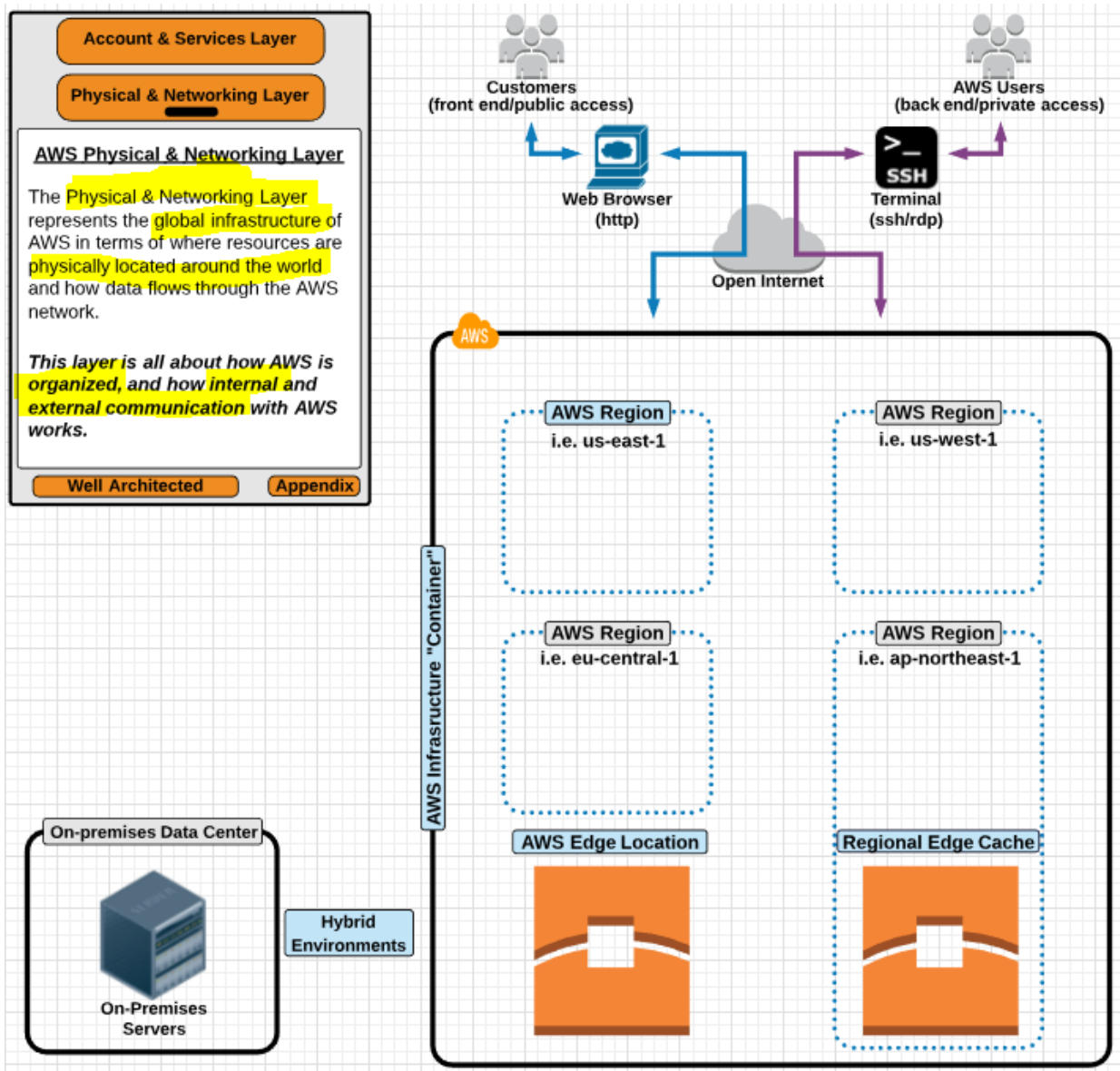
AWS Global Infrastructure

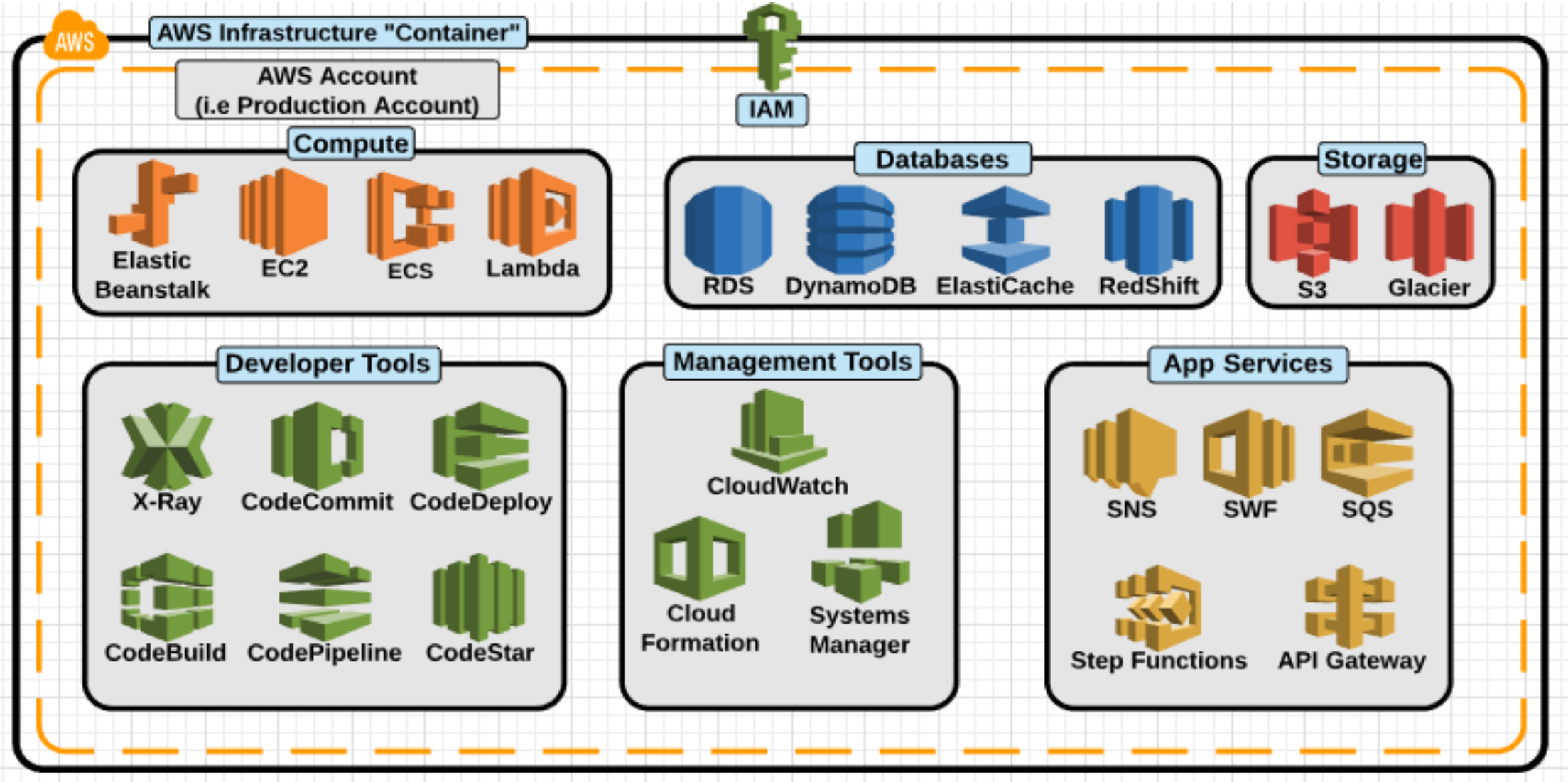
By

Keshav Kummari

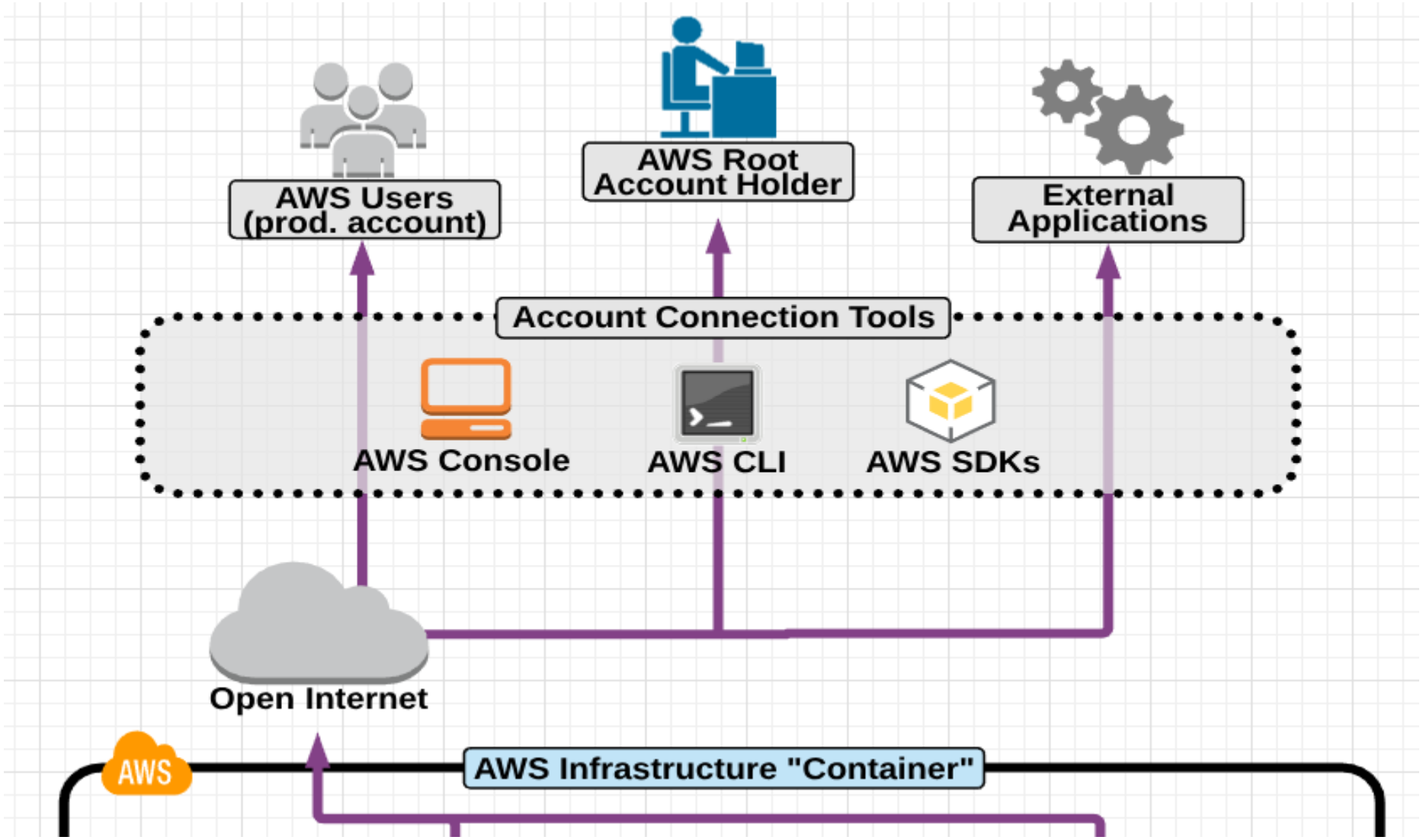

Account & Services Layer
Physical & Networking Layer
AWS Account and Services Layer
The Account and Services Layer represents how you create, access, and manage an AWS account and its services. From how you interact with an AWS account and managing user rights, to how you access and use various AWS services and features.
This layer is all about account management and managing services.
Well Architected
Appendix
AWS Users (prod. account)
AWS Root Account Holder
AWS Users (dev. account)
Account Connection Tools
AWS Console
AWS CLI
AWS SDK
Open Internet
Open Internet
AWS
AWS Infrastructure "Container"
IAM
IAM
AWS Account (i.e. Production Account)
Cross Account Access
AWS Account (i.e. Development Account)
On-premises Data Center
On-Premises Servers
Hybrid Environments


Account & Services Layer
Physical & Networking Layer
AWS Physical & Networking Layer
The Physical & Networking Layer represents the global infrastructure of AWS in terms of where resources are physically located around the world and how data flows through the AWS network.
This layer is all about how AWS is organized, and how internal and external communication with AWS works.
Well Architected
Appendix
Customers
(front end/public access)
AWS Users
(back end/private access)
Web Browser
(http)
SSH
Terminal
(ssh/rdp)
Open Internet
AWS
AWS Region
i.e. us-east-1
AWS Region
i.e. us-west-1
AWS Region
i.e. eu-central-1
AWS Region
i.e. ap-northeast-1
AWS Infrasructure "Container"
AWS Edge Location
Regional Edge Cache
On-premises Data Center
On-Premises
Servers
Hybrid
Environments

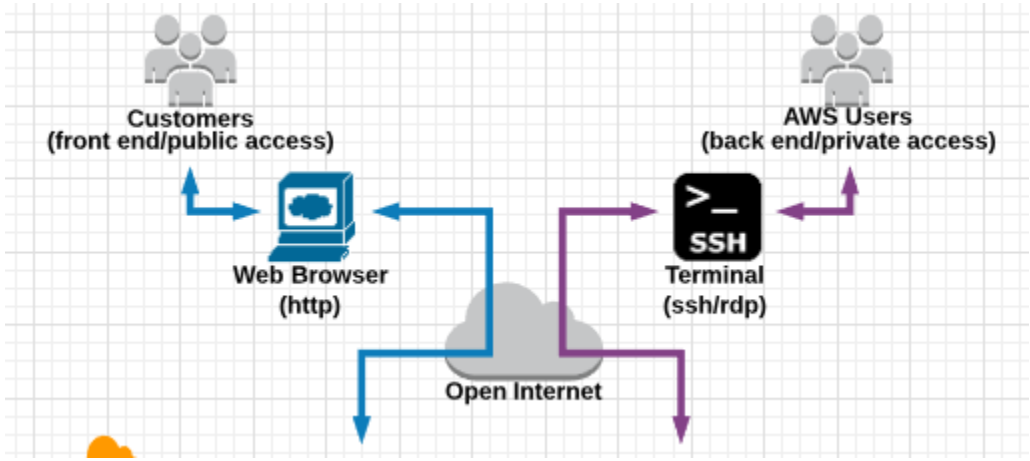
AWS Infrastructure Container

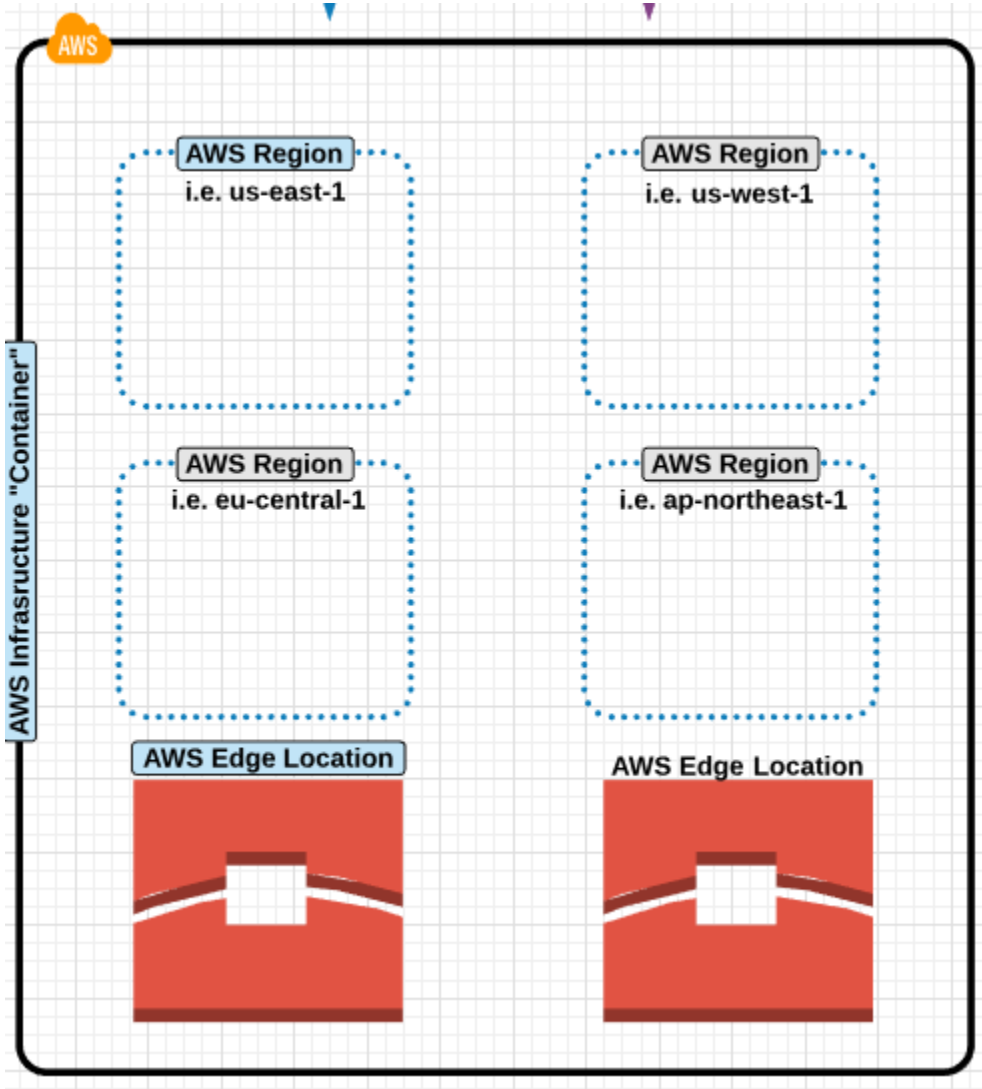


Connecting to AWS Cloud Using Various Ways

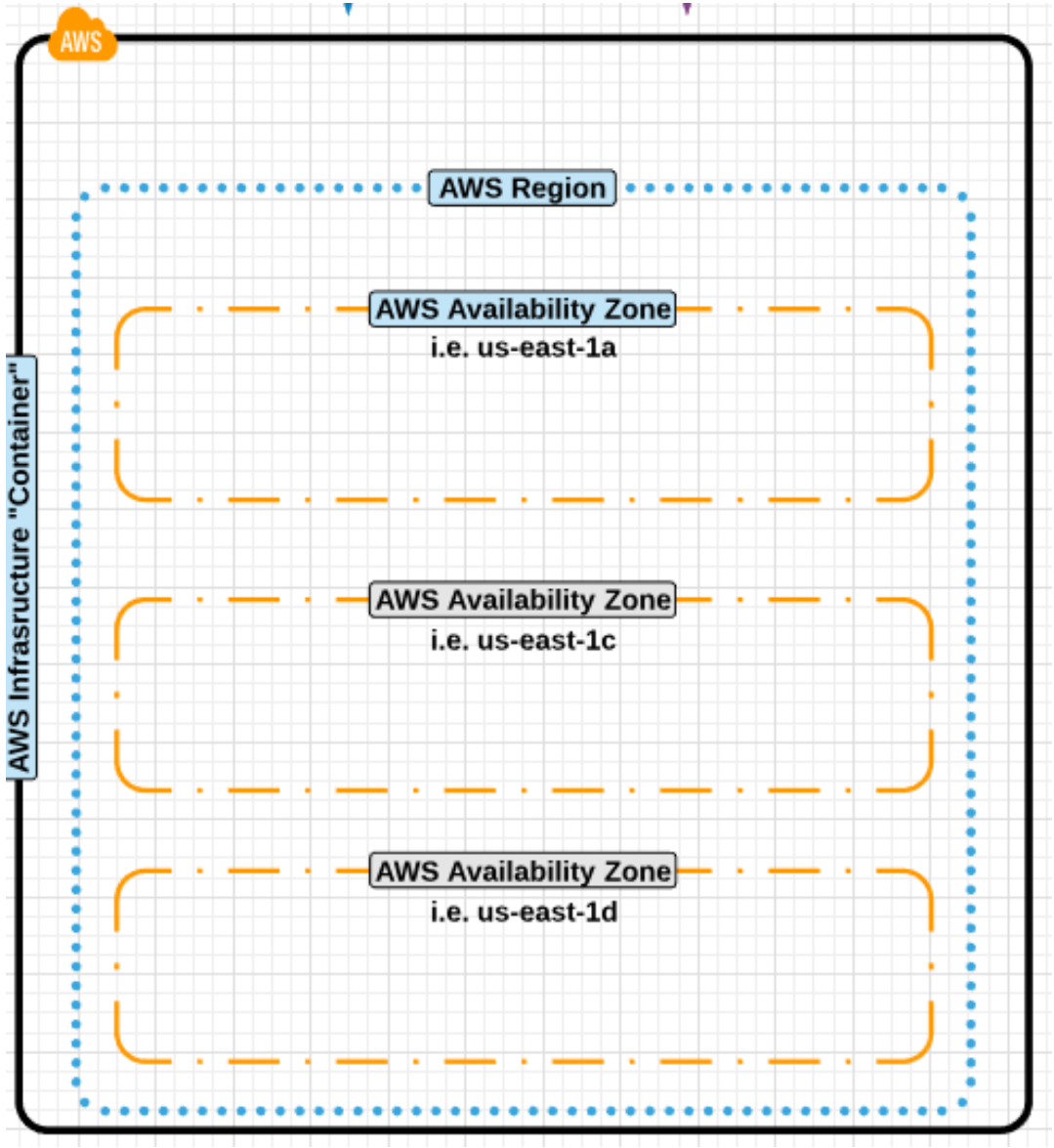


AWS Global Infrastructure





Region & Availability Zones



AWS Regions

- AWS is made up of regions which are a grouping of independently separated data centers in a specific geographic regions known as “Availability Zones”.

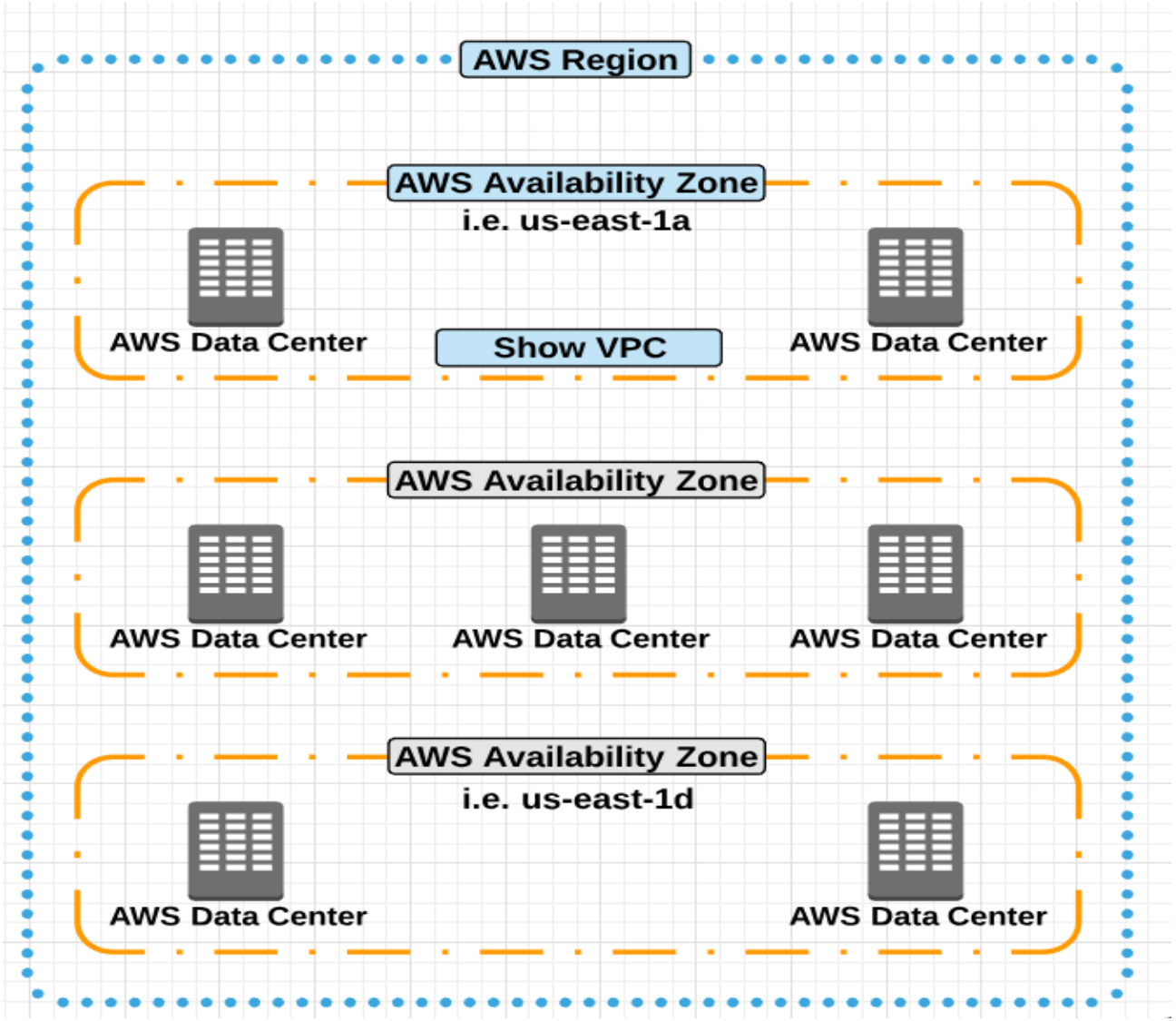
- Availability of regions allows the architect to design applications to conform to specific laws and regulations for specific parts of the world.

- When viewing a region in the console you will only view resources in one region at a time but they will be across all AZ’s within that region.

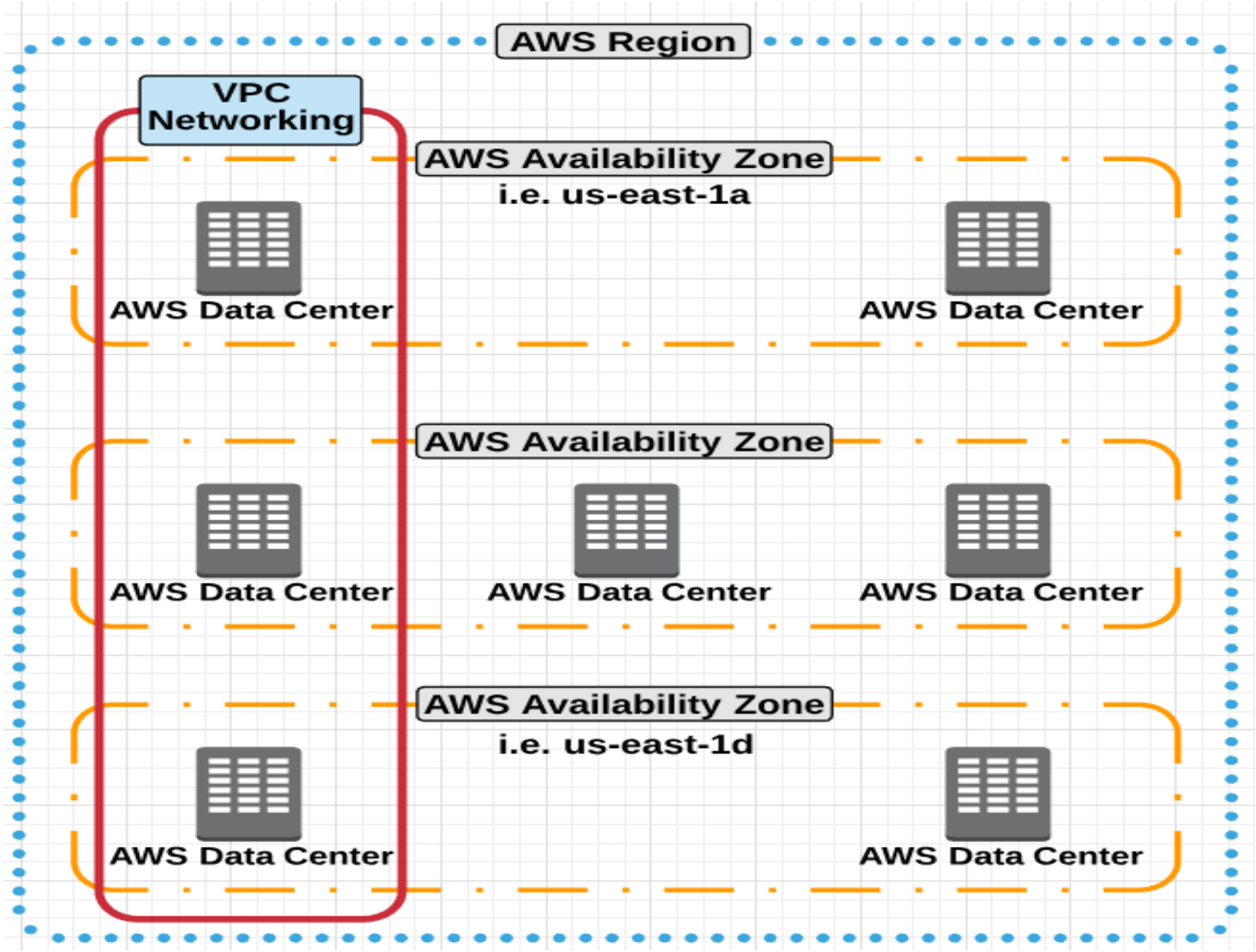
- Some AWS services work “Globally” and not within a specific region.
  - For Example : Users are created in IAM will work across regions.

Regions & Availability Zones Map

Region & Availability Zones Details



VPC


AWS Region
VPC Networking
AWS Availability Zone
i.e. us-east-1a
AWS Data Center
AWS Data Center
AWS Availability Zone
AWS Data Center
AWS Data Center
AWS Data Center
AWS Availability Zone
i.e. us-east-1d
AWS Data Center
AWS Data Center

VPC Essentials

"Amazon Virtual Private Cloud (Amazon VPC) enables you to launch Amazon Web Services (AWS) resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own datacenter, with the benefits of using the scalable infrastructure of AWS" – Amazon Web Services

A VPC is designed to resemble:

- Private on-premise data centers
- Private corporate network

Private network features available in AWS VPCs:

- Private and Public subnets
- Scalable architecture
- Ability to extend corporate/on-premise network to the cloud as if it was part of your network (VPN)

Important VPC Facts:

- A VPC is housed within a chosen AWS region.
- A VPC spans multiple availability zones within a region.
    - This allows you to provision redundant resource in separate availability zones while having them accessible on the same network (foundation of high availability and fault tolerant architecture).
- AWS provides a DNS server for your VPC so each instance has a hostname. However, you can run your own DNS servers by changing the DHCP option set configuration within the VPC.

Benefits of VPC

- Ability to launch instances into a subnet.
- Ability to define custom CIDR (IP address range) inside each subnet.
- Ability to configure routes between subnets via route tables.
- Ability to configure an internet gateway to provide a route to the internet for resources launched inside the VPC.
- Ability to create a layered network of resources.
- Ability to extend your on-premise network into the cloud with VPN/VPG and an IPsec VPN tunnel.
- Layered Security:
  - Instance level Security Groups (firewall on the instance level)
  - Subnet level network ACLs (firewall on the subnet level)

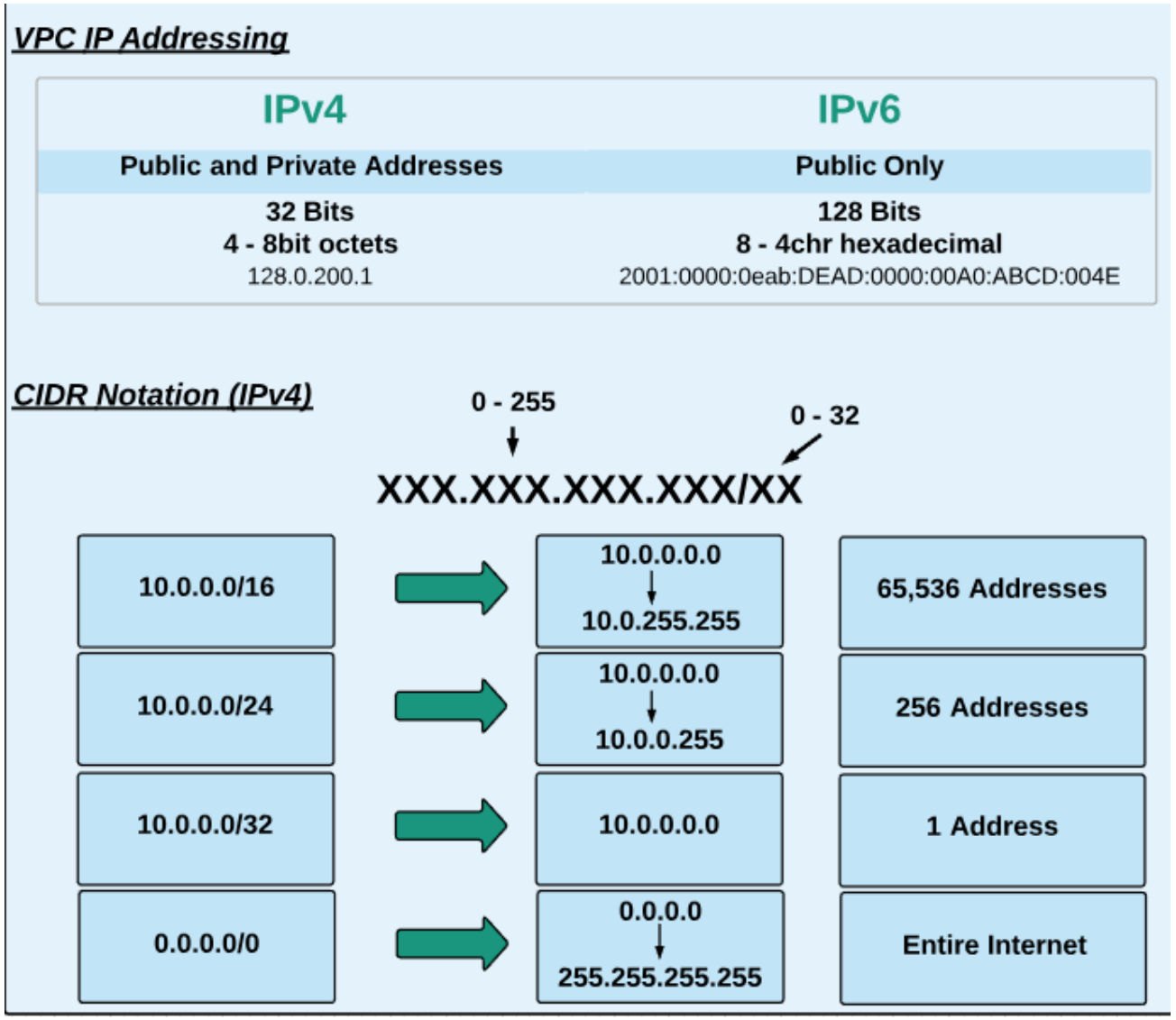
Default VPC

- The default VPC is the VPC that comes preconfigured in your AWS account when it is first created.
- The default VPC has a different setup than a non-default VPCs.
- The default VPC is meant to allow the user easy access to a VPC without having to configure it from scratch.
- In the default VPC, all subnets have a route to the internet via route table and an attached IGW.
- Each instance launched in the default VPC (by default) has a private and public IP address (defined on the subnet settings).

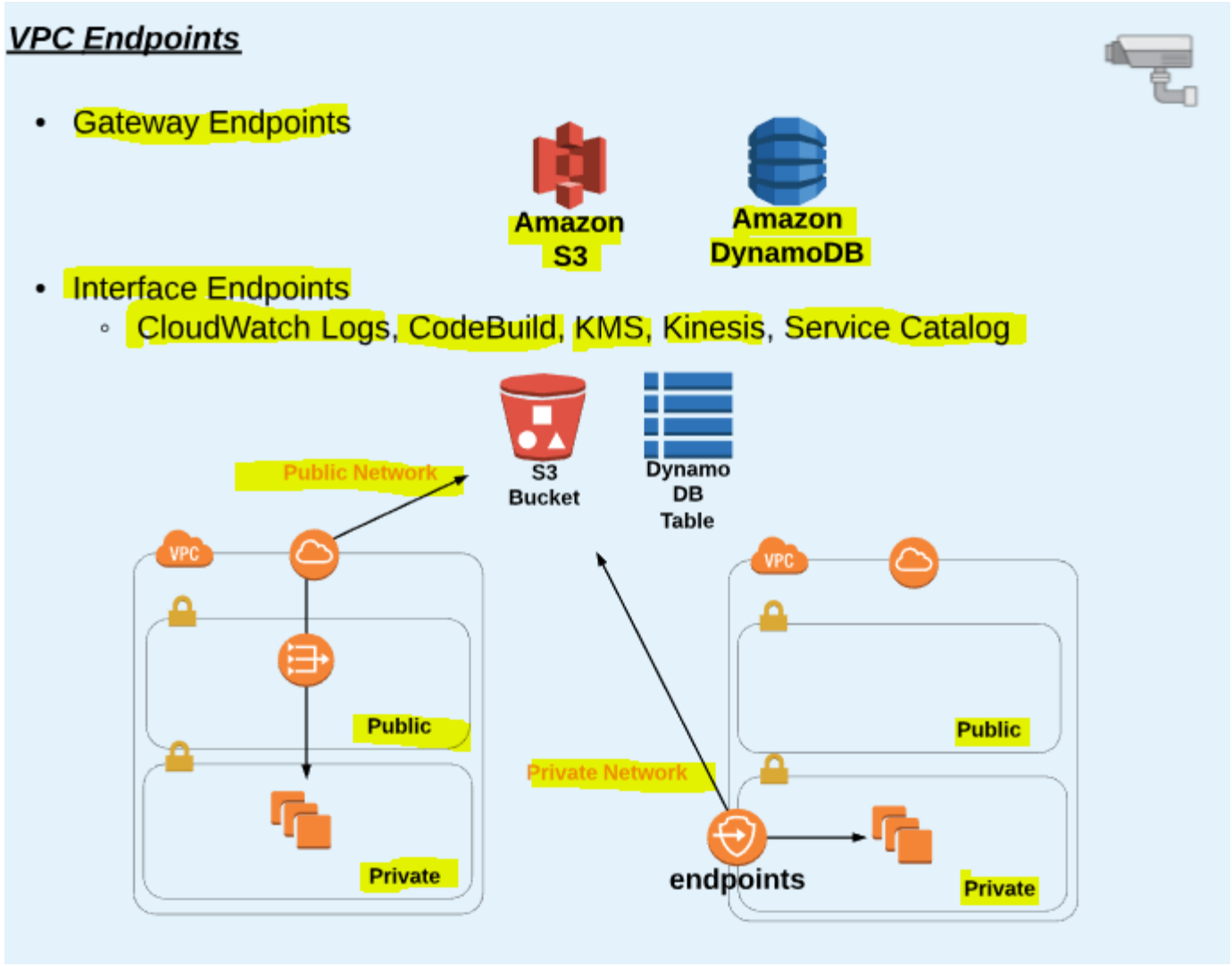
VPC Limits

- 5 VPCs per region (more available upon request)
- 5 internet gateways per region (this is equal to your VPC limit because you can only have one internet gateway attached to a VPC at a time)
- 50 customer gateways per region
- 50 VPN connections per region
- 200 route tables per region / 50 entries per route table
- 5 elastic IP addresses
- 500 security groups per VPC
- 50 rules per security group
- 5 security groups per network interface (security groups although generally referred to as being on the on the instance level are technically on the VPC level)

CIDR – Class-Less Inter Domain Routing



VPC Endpoints



Internet Gateway: IGW

Internet Gateway:

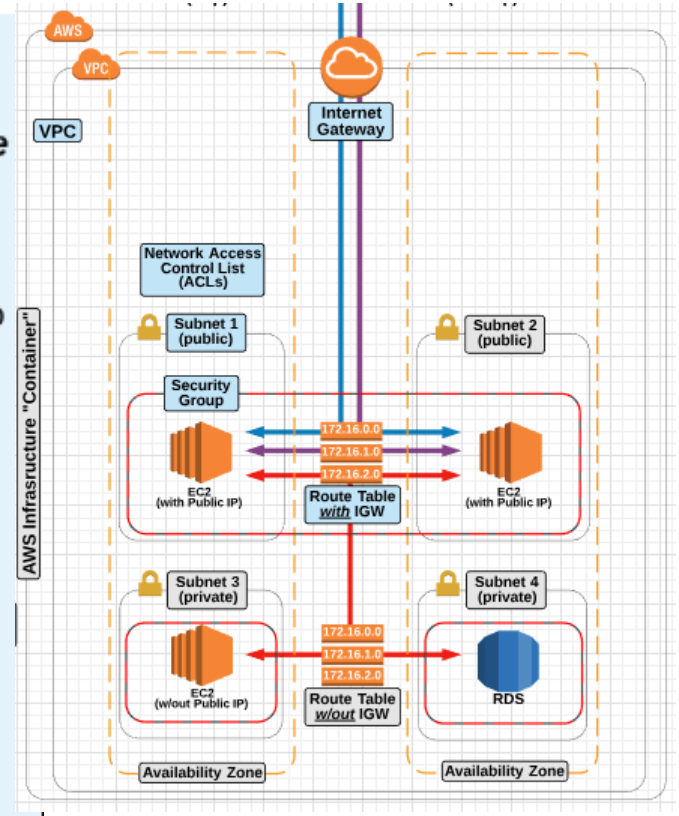
- Is a VPC component that ***allows communication between instances in your VPC and the Internet***.
- Is a horizontally scaled, ***redundant and highly available.***
- It imposes no availability risks or bandwidth constraints on your network traffic.
- Provides NAT translation for instances that have a public IP addresses assigned (public IP to private IP).

NOTE: Your "default" VPC already has an IGW ***attached***.

Internet Gateway rules and details you need to know:

- Only 1 IGW can be attached to a VPC at a time.
- An IGW cannot be detached from a VPC while there are active AWS resources in the VPC with Public or Elastic IPs
- An IGW must be attached to a VPC if the resources inside the VPC need to connect to resources via the open internet.

"To enable access to or from the internet for instances in a VPC subnet, you must attach an Internet gateway to your VPC, ensure that your subnet's route table points to the Internet Gateway, ensure that instances in your subnet have a public IP address or Elastic IP address, and ensure that your network access control and security group rules allow the relevant traffic to and from your instance" – AWS



Route Tables - RTB

Route Tables:

"A route table contains a ***set of rules***, called ***routes***, that are used to ***determine where network traffic is directed***." - Amazon web Services

- A route table's rules are comprised of two main components:
  - ***Destination***: The CIDR block range of the *target* (where the data is routed to).
  - ***Target***: A name identifier of where the data is being routed to.

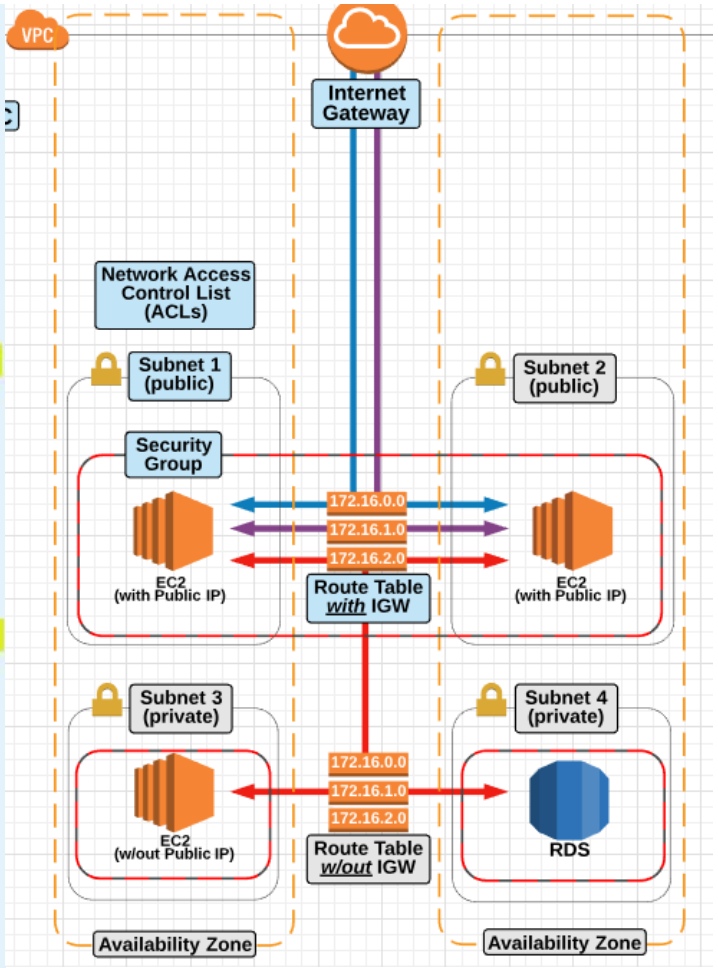
- By default, all subnets traffic is allowed to each other available subnet within your VPC which is called the local route.
- You cannot modify the local route

- Unlike an IGW, you can have multiple "active" route tables in a VPC
- You cannot delete a route table if it has ***"dependancies"*** (associated subnets)

Best practice is to leave the default route table and create a new route table when new routes are needed for specific subnets.

NOTE: The "default" VPC already has a ***"main"*** route table.

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	igw-95d589f2



Subnets

"When you create a VPC, it spans all of the Availability Zones in the region. After creating a VPC, ***you can add one or more subnets in each Availability Zone***. Each subnet ***must reside entirely*** within one Availability Zone and ***cannot span zones***." -Amazon Web Services

- Subnets MUST be associated with a route table.
- A ***PUBLIC*** subnet ***HAS*** a route to the Internet.
  - It is associated with a route table that has an IGW attached.
- A ***PRIVATE*** subnet ***does NOT have*** a route to the Internet.
  - It is associated with a route table that does NOT have an IGW attached.

- Instances launched into a ***private subnet*** can't communicate with the internet.
  - This creates a higher level of security, but it creates a limitation of an instance not being able to download software and/or updates.
  - This issue is solved by routing traffic through a NAT instance.

- By default all subnets traffic is allowed to each other available subnet within via the ***local*** target in the route table.
- A subnet is located in one specific availability zone, and does not span AZs.

NOTE: The "default" VPC already has subnets created and associated with a route table.

NACL - Essentials

- ACLs Operate at the network/subnet level.
- They support ***allow*** AND ***deny*** rules for traffic traveling into or out of a subnet.
- They are ***stateless***: so return traffic must be allowed through an ***outbound rule***.

- They process rules in number order when deciding whether to allow traffic.
- Rules are evaluated in order, starting with the lowest rule number - for example:
  - If traffic is denied at a lower rule number and allowed at a higher rule number, the allow rule will be ignored and the traffic will be denied.
- The last rule in every ACL is a "catch all" deny rule.
  - This means that unless a protocol/port is explicitly allowed, it will be denied.

- A network access control list (NACL) is an ***optional layer of security*** for your VPC that acts as a ***firewall*** for controlling traffic in and out of one or more ***subnets***.

- ***Best practice*** to increment numbers by 10 so if you have to place in a rule in a certain order it does not create an issue

Inbound

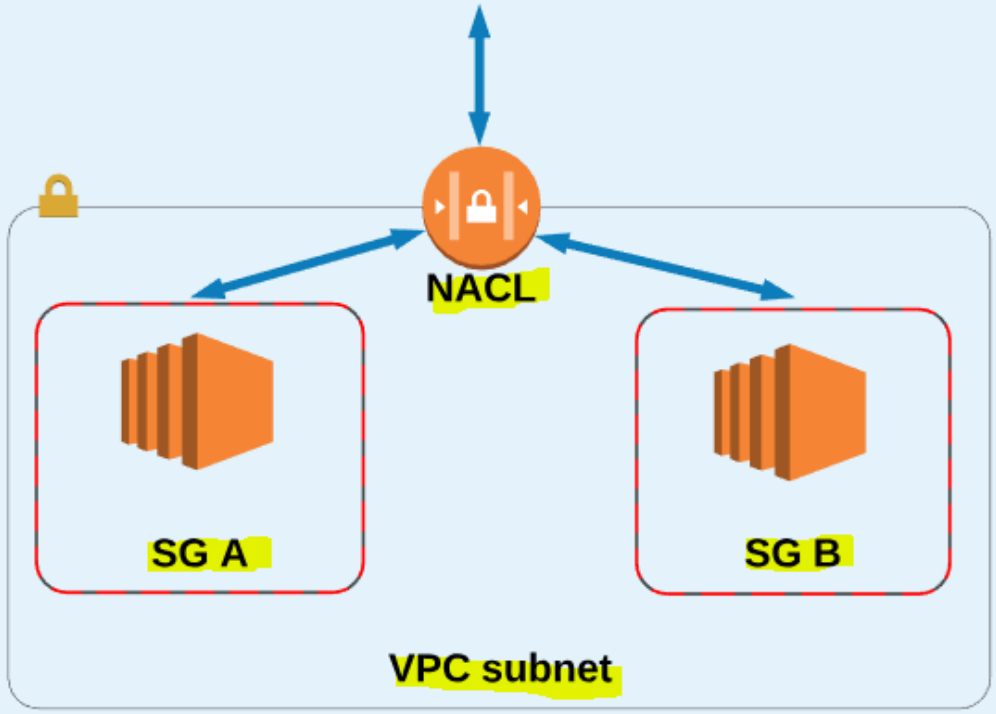
Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
120	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
130	Custom TCP Rule	TCP (6)	32768-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound

Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
100	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
110	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
120	Custom TCP Rule	TCP (6)	1024-65535	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

NACL Rules

- Rules are evaluated from **lowest to highest based on "rule #"**.
- The first rule found that applies to the traffic type is immediately applied, regardless of any rules that come after it (have a higher "rule #").
- A subnet can only be associated with ONE NACL as a time.
- An NACL allows or denies traffic from entering a subnet. Once inside the subnet, other AWS resources (i.e. EC2 instances) may have an additional layer of security (security groups).



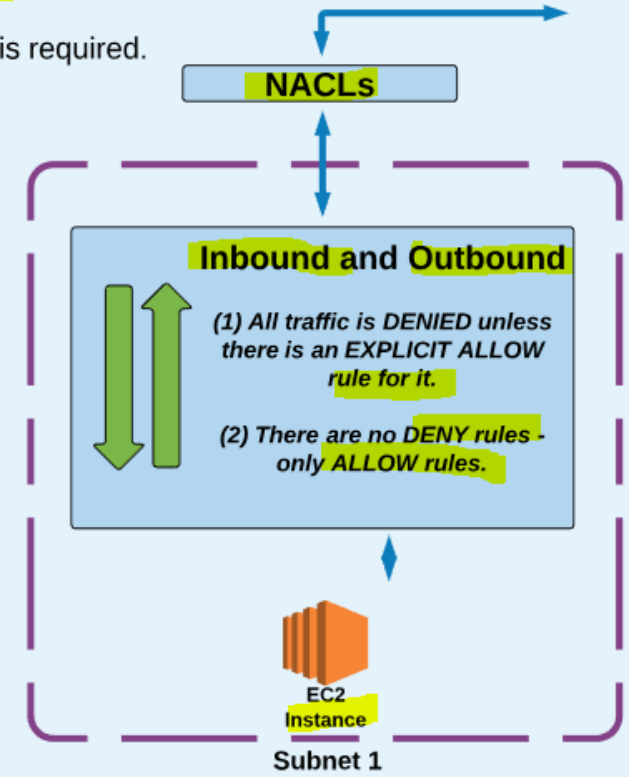
Security Groups

Security Groups:

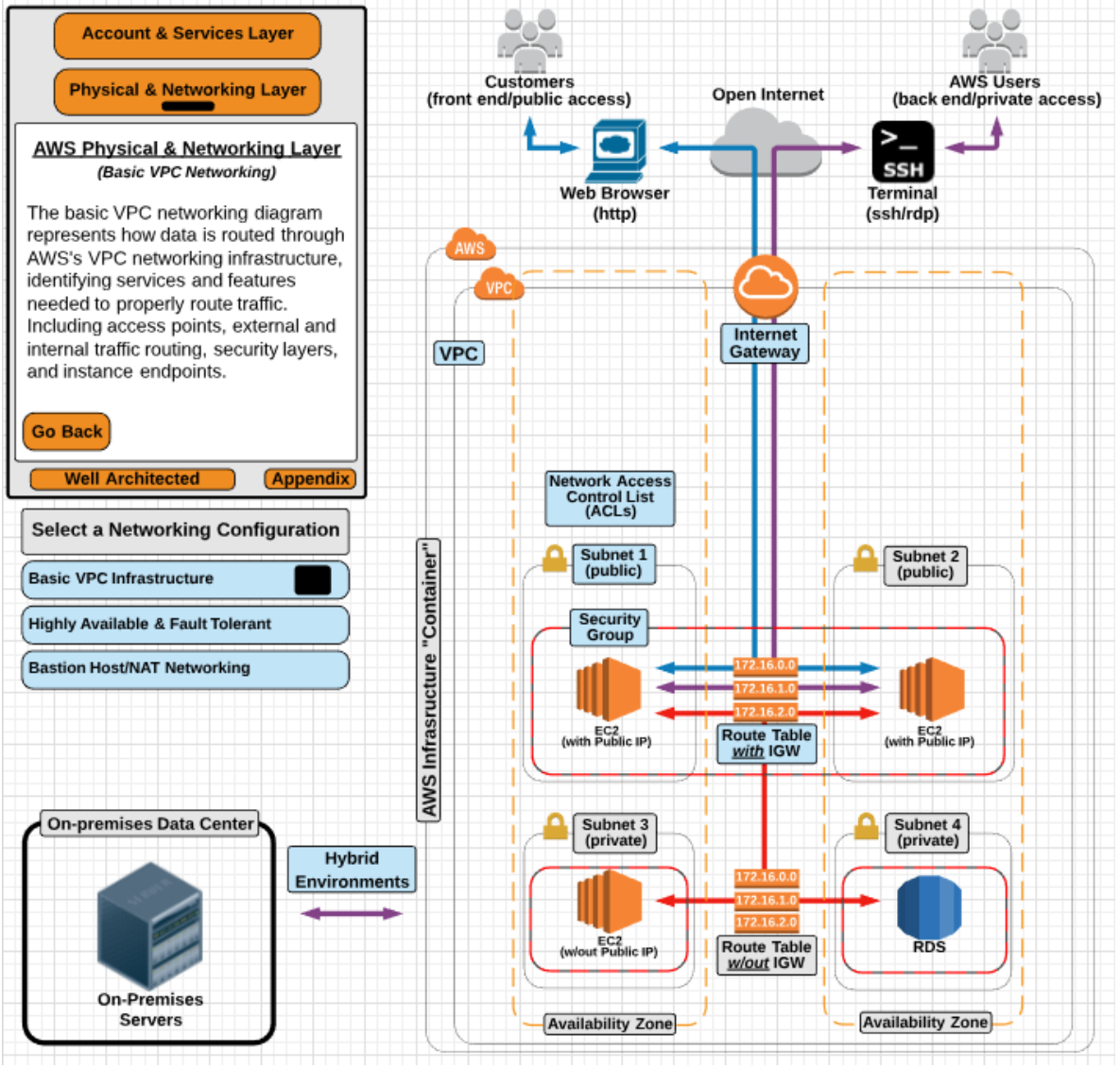
- Security groups are very similar to NACLs in that they ***allow/deny traffic***.
- However, security groups are security for the ***instance level*** (as opposed to the subnet level with ALCs).
- In addition, the way ***allow/deny "rules" work are different from ACLs***:
  - Security groups support only allow rules.
  - They are ***stateful***: so return traffic requests are allowed regardless of rules.
  - All rules are evaluated before deciding to allow traffic.

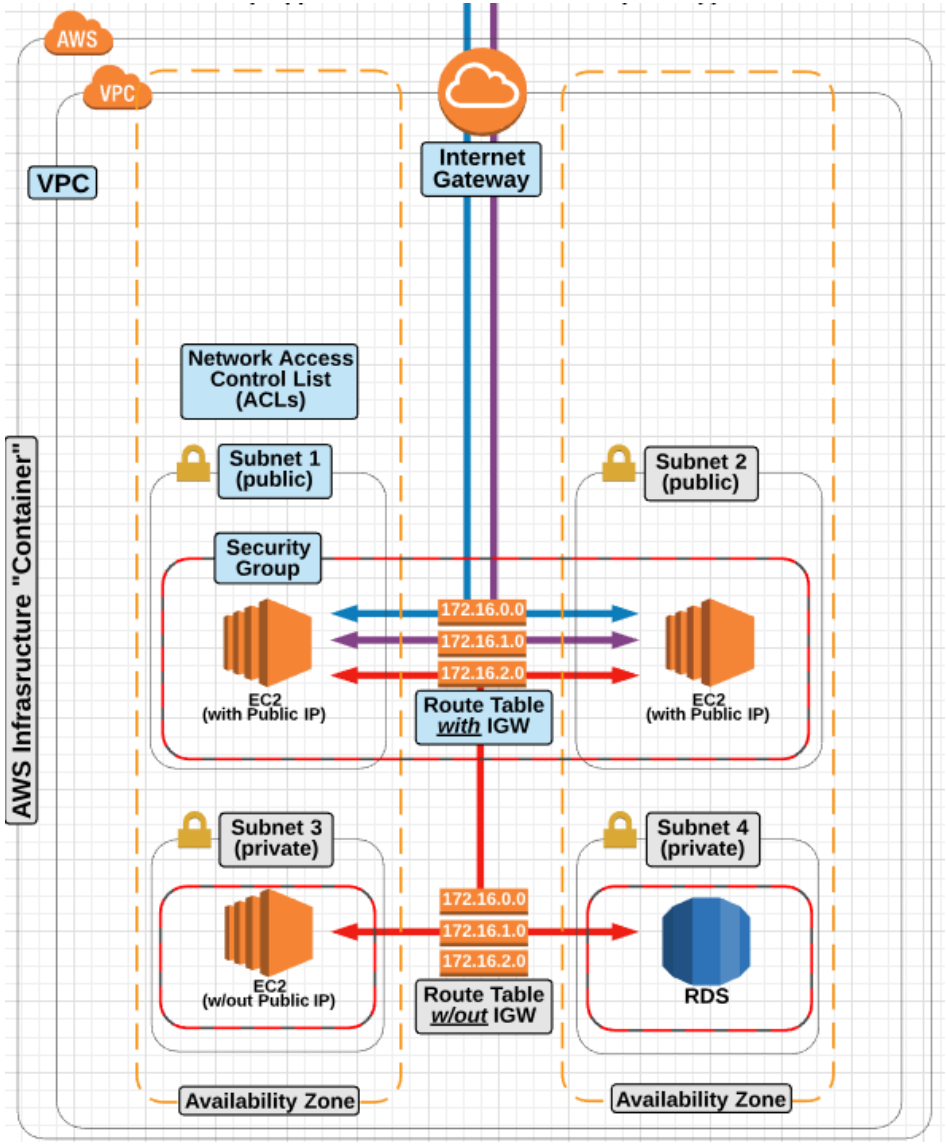
NOTE: Best practice is to allow ONLY traffic that is required.

Type	Protocol	Port Range	Source
SSH (22)	TCP (6)	22	0.0.0.0/0
HTTP (80)	TCP (6)	80	0.0.0.0/0

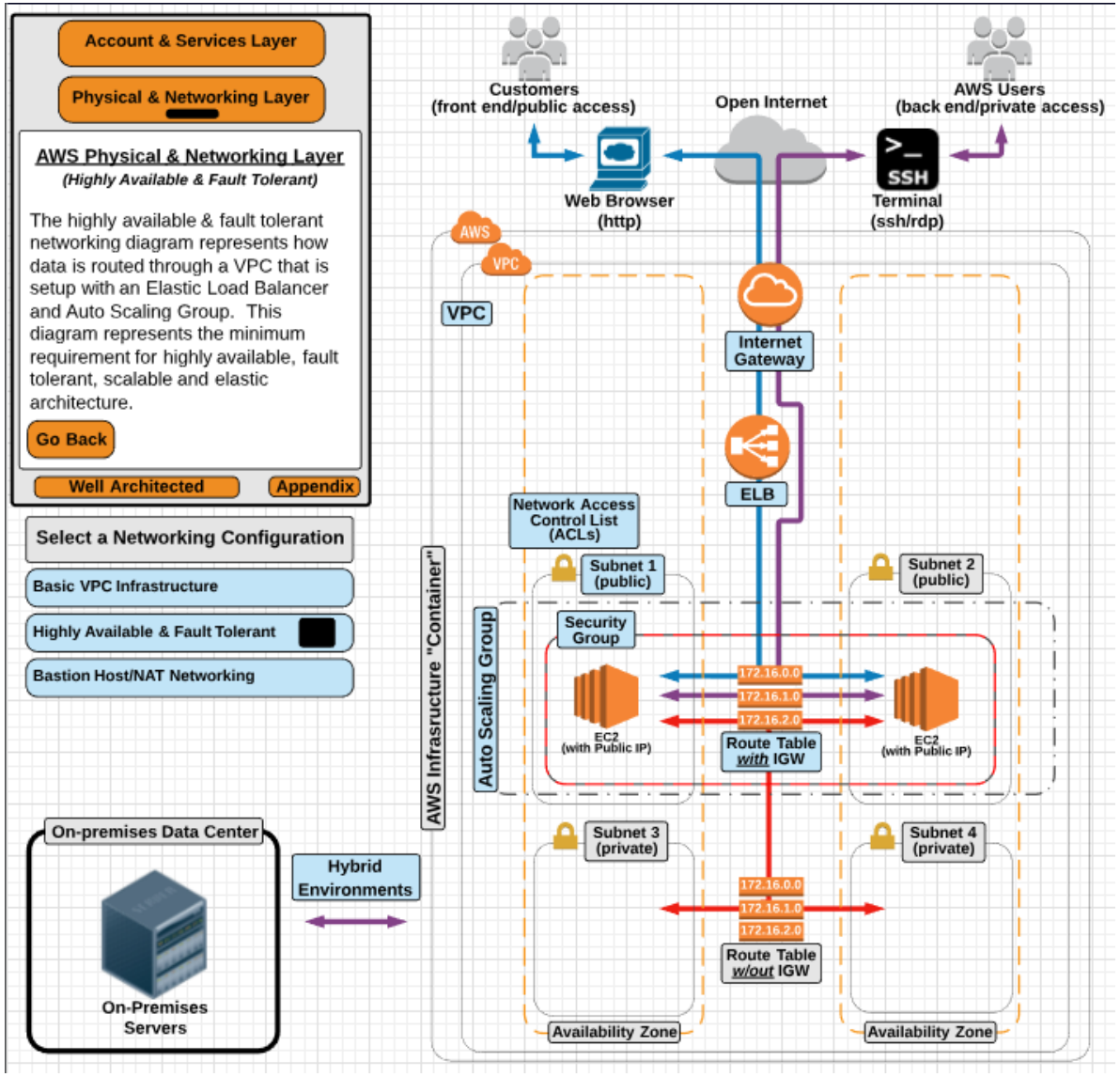


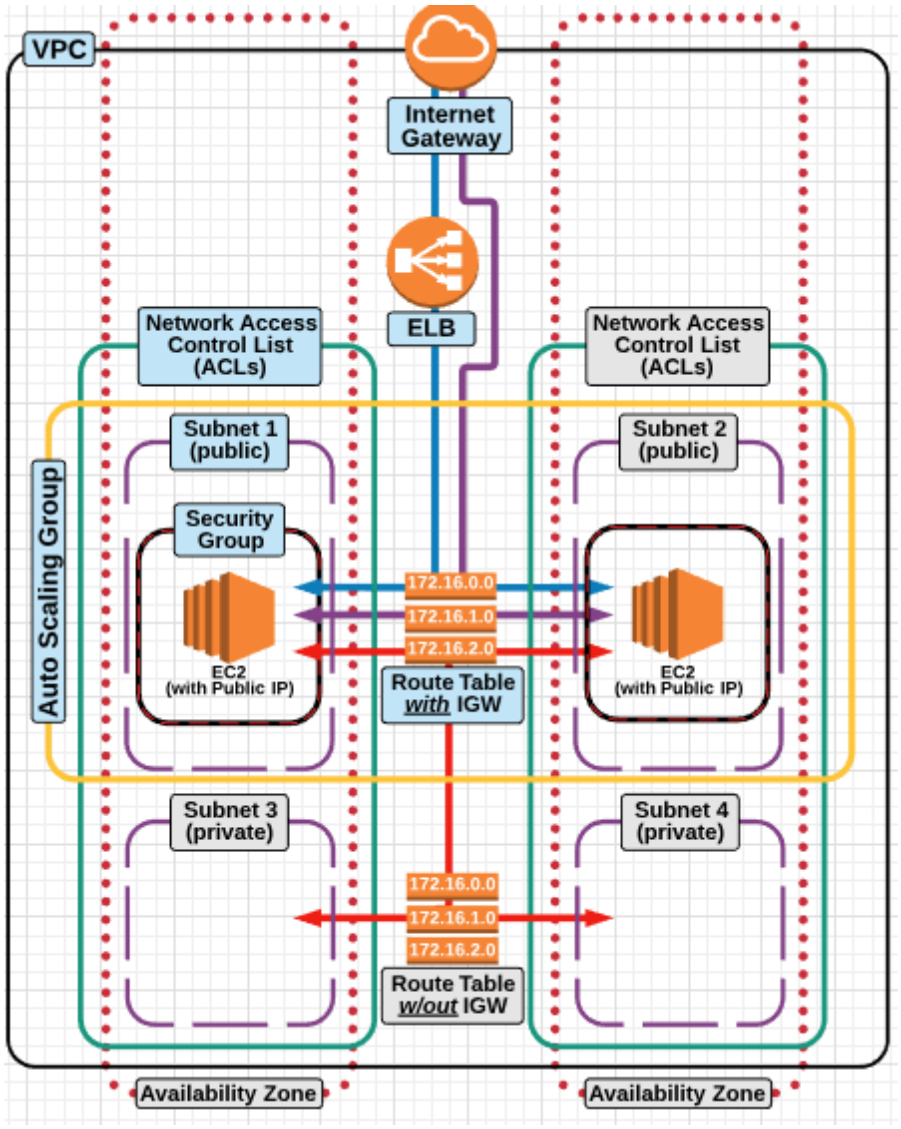
Basic VPC Infrastructure



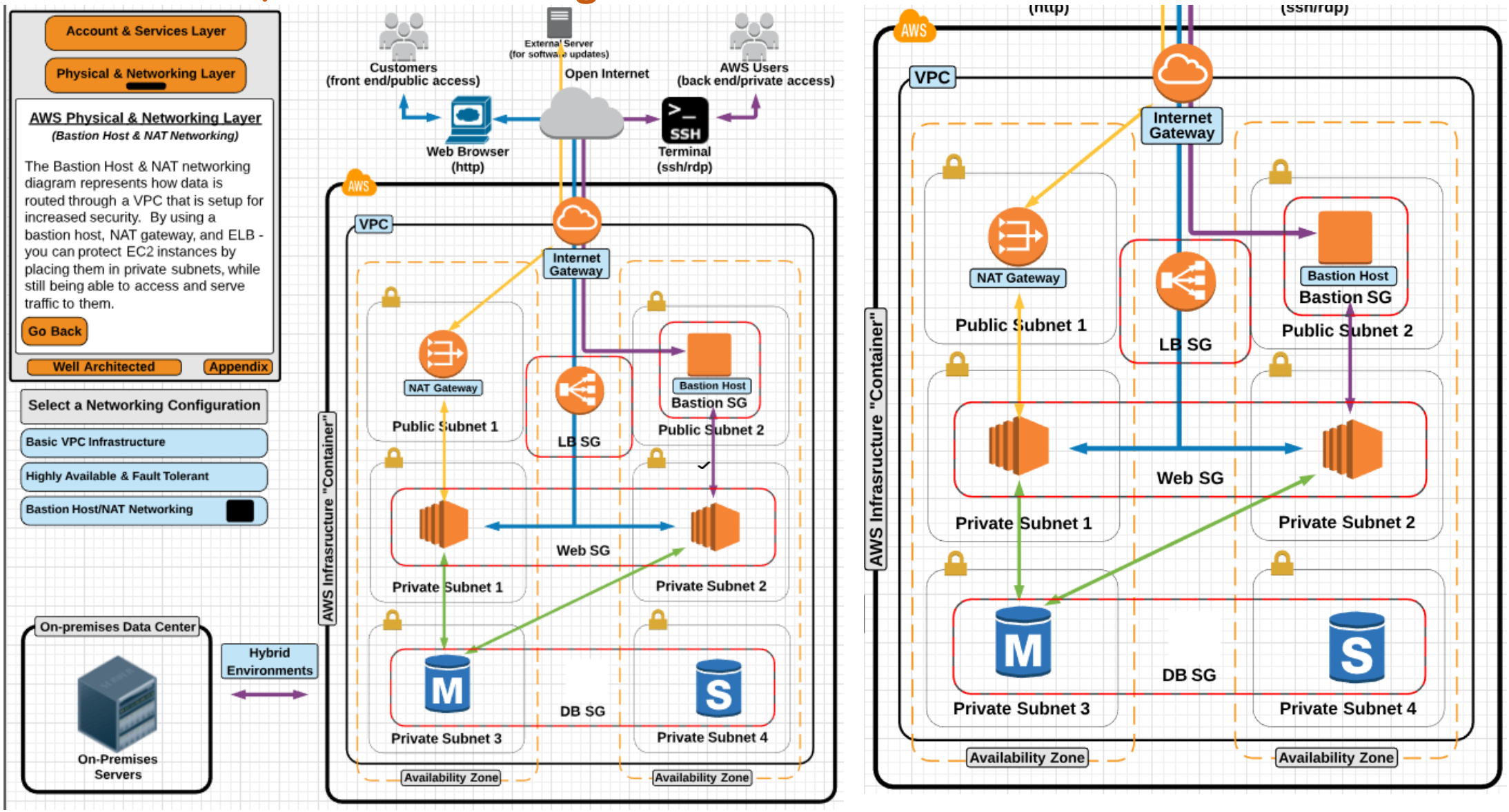


Highly Available & Fault Tolerant

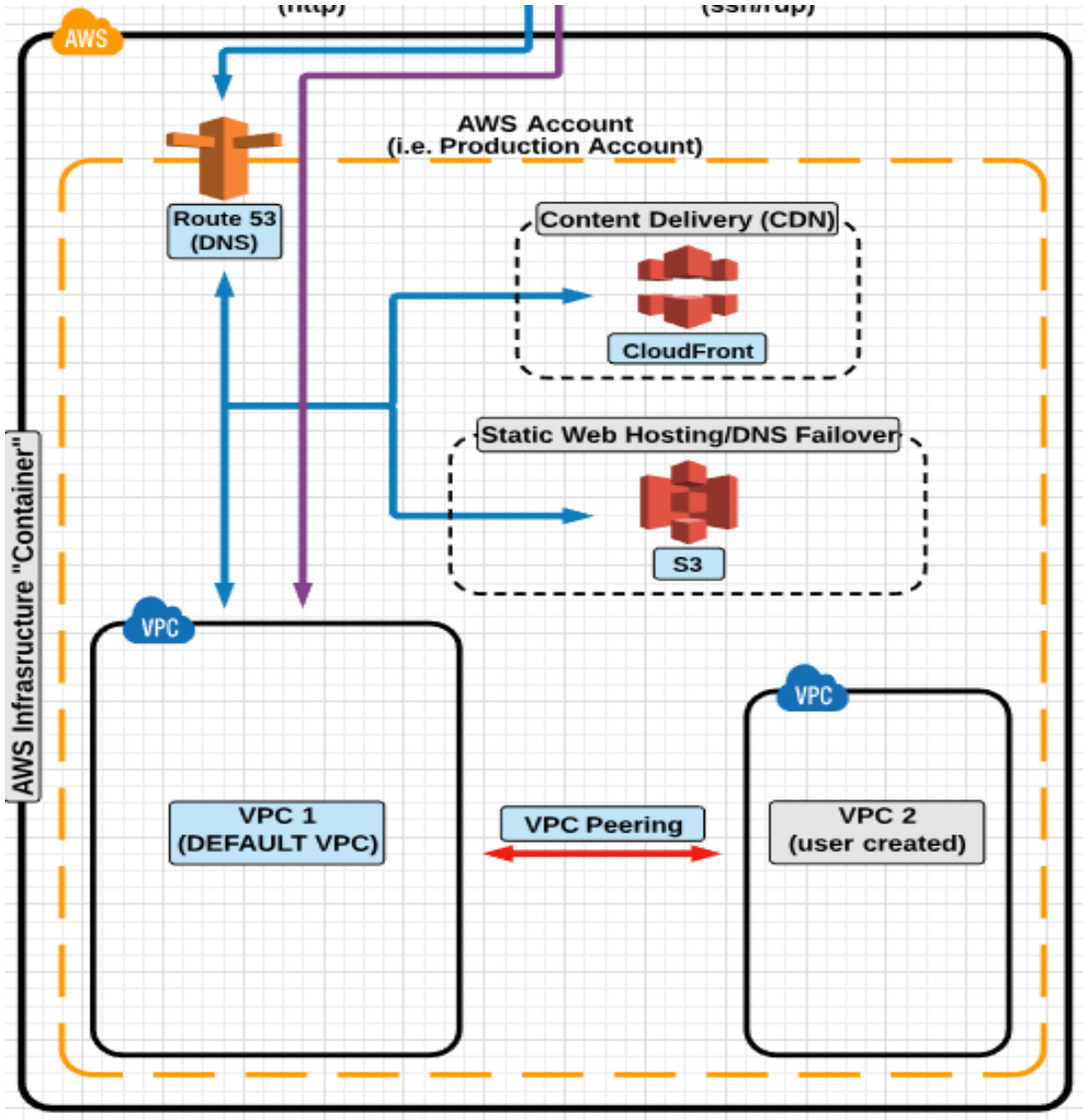




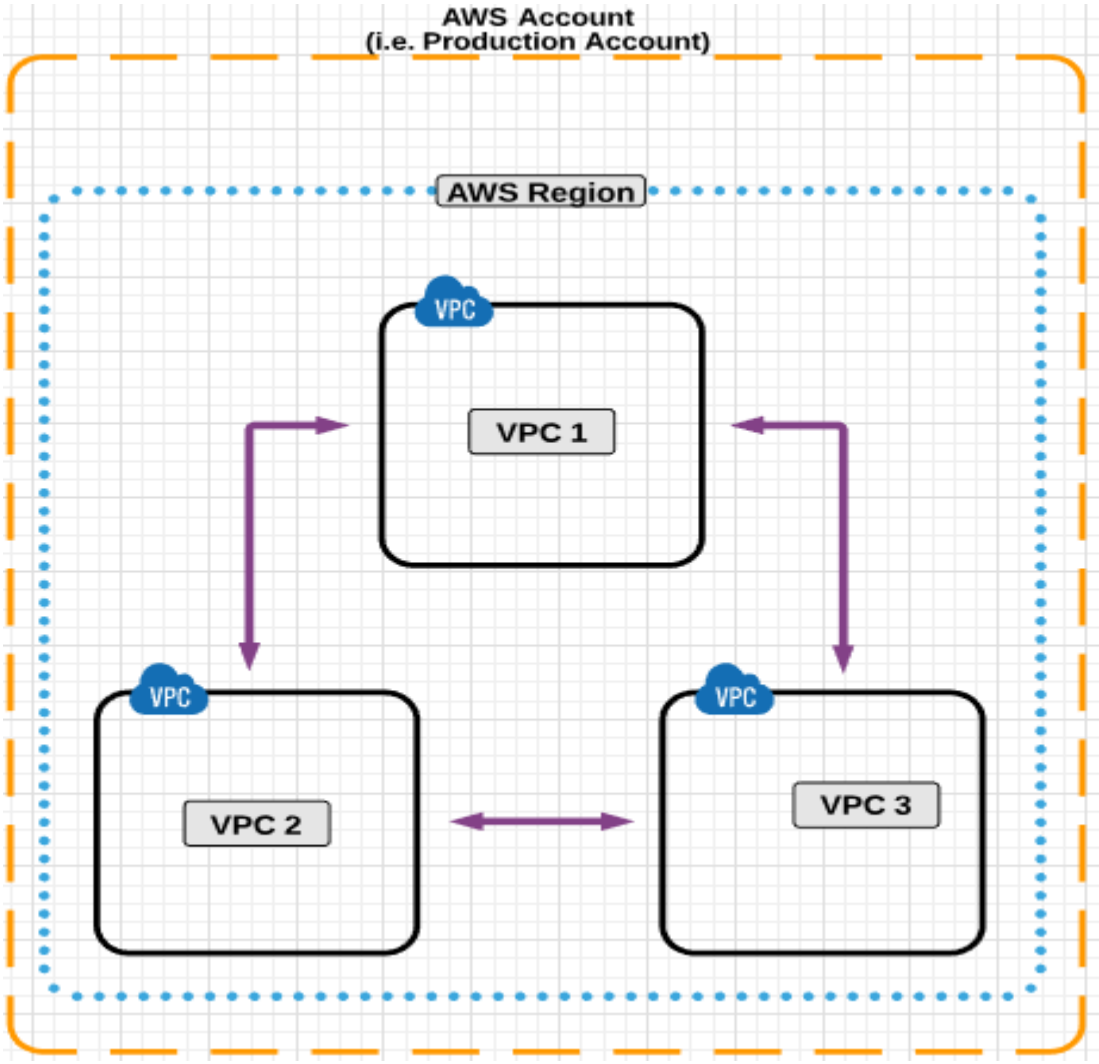
Bastion Host/NAT Networking



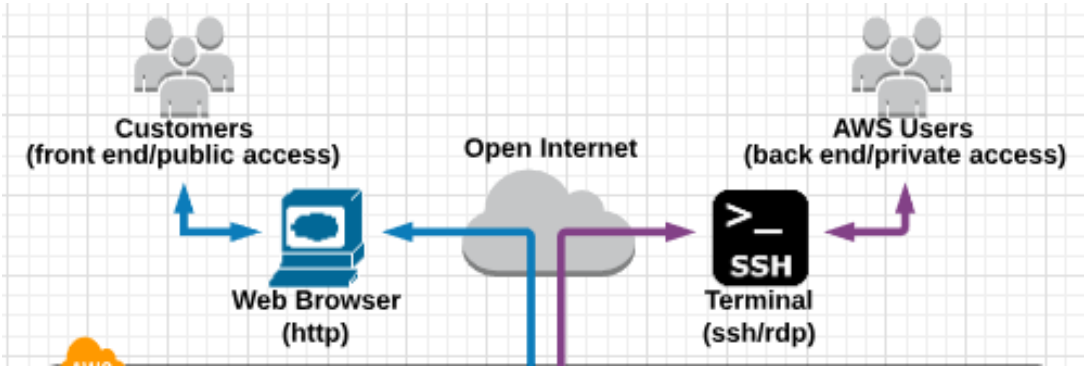
VPC & VPC Peering

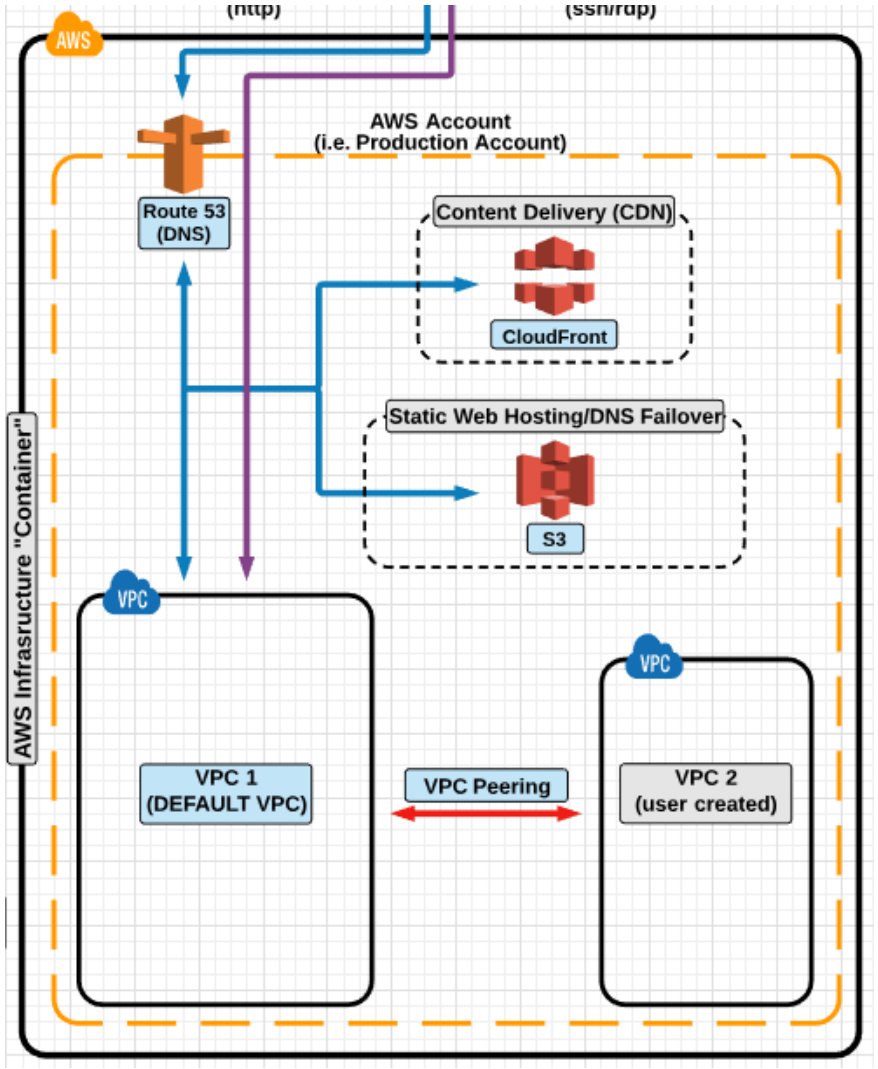


VPC Peering

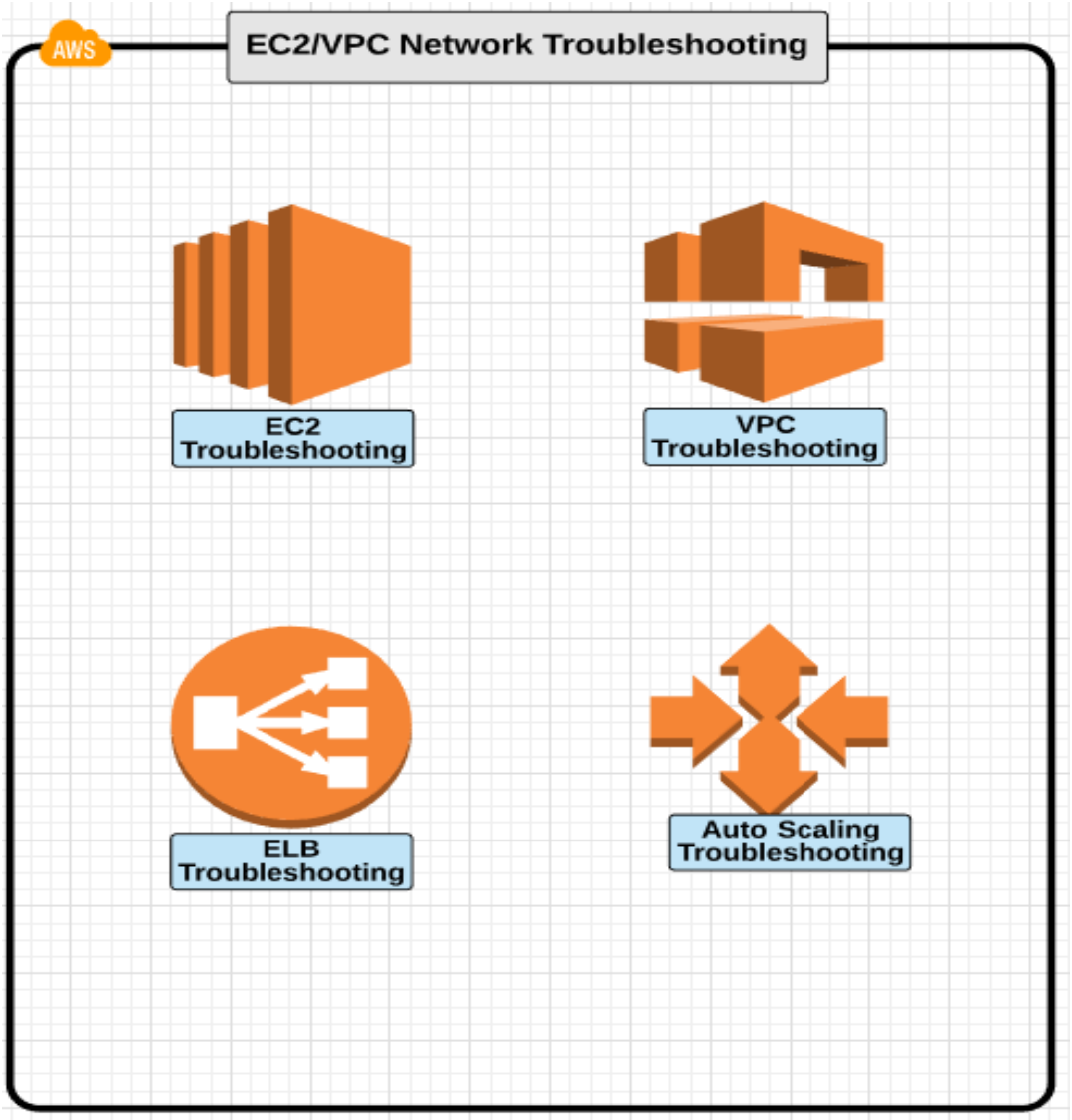

AWS Account
(i.e. Production Account)
AWS Region
VPC
VPC 1
VPC
VPC 2
VPC
VPC 3

Connect a VPC Using Various ways

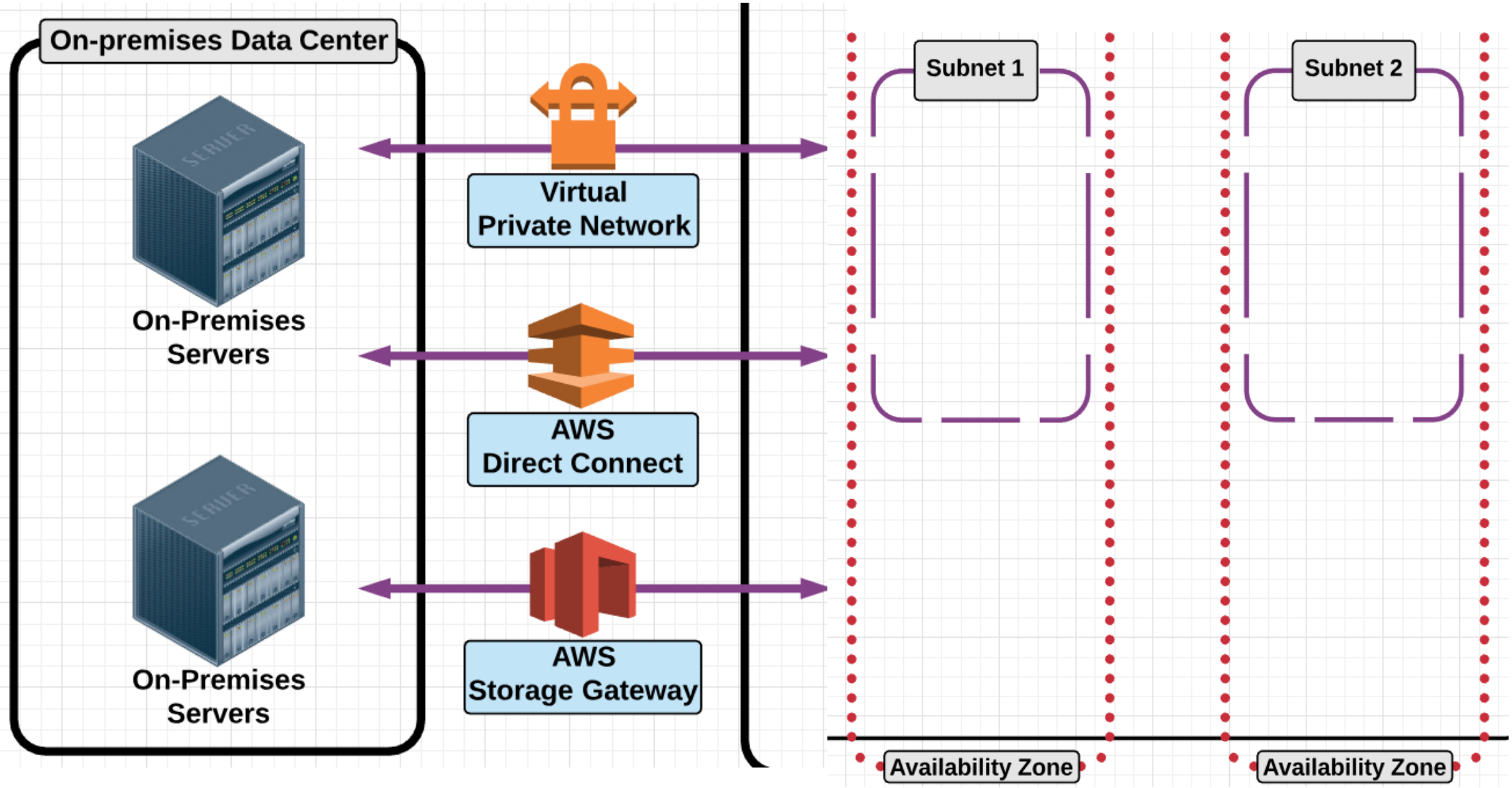




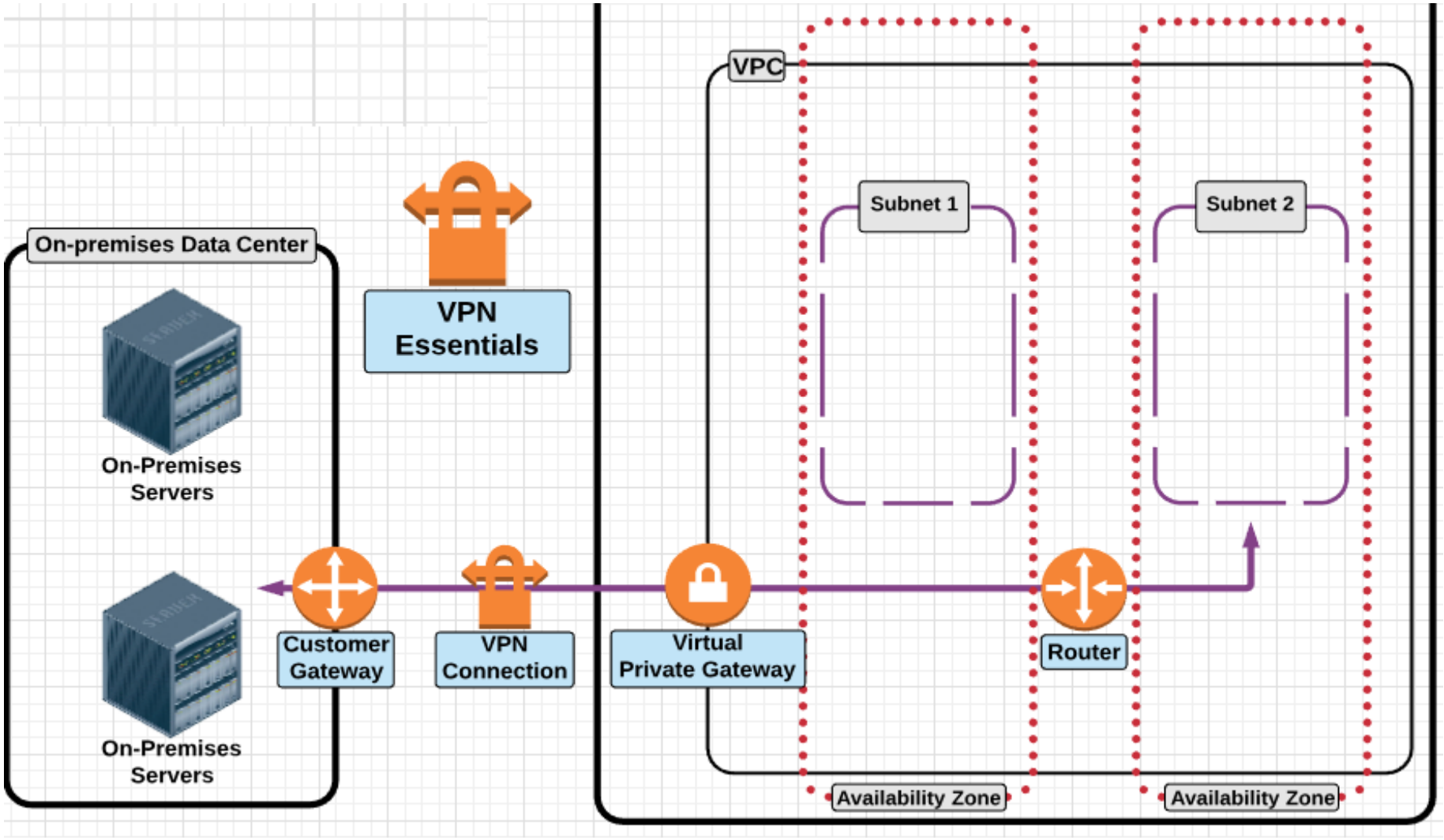
Troubleshooting



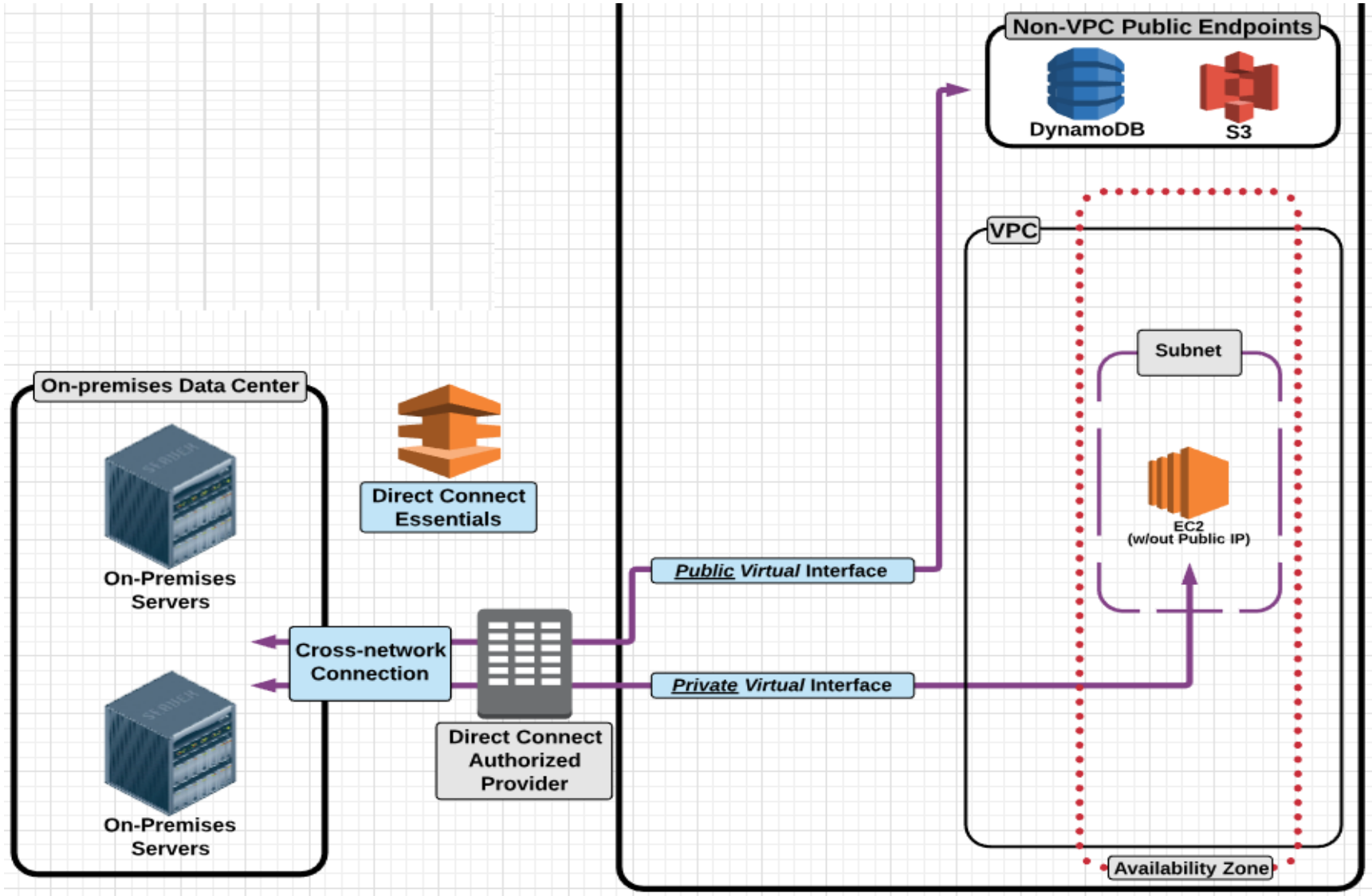
Connect On-Premises Data Center With AWS Cloud



Connect On-Premises Data Center Using VPC



Connect On-Premises Data Center Using Direct Connect



Connect On-Premises Data Center Using Storage Gateway