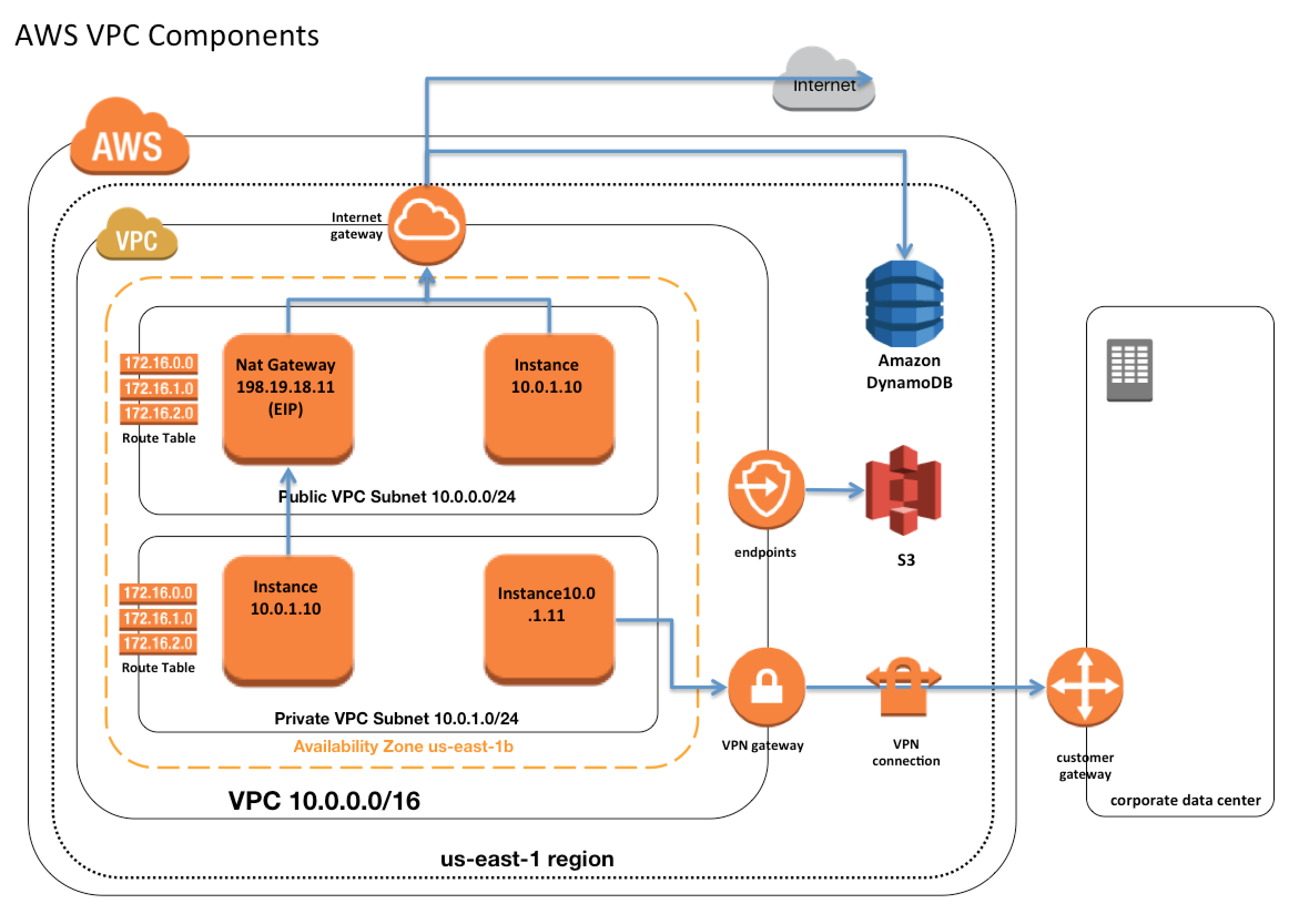
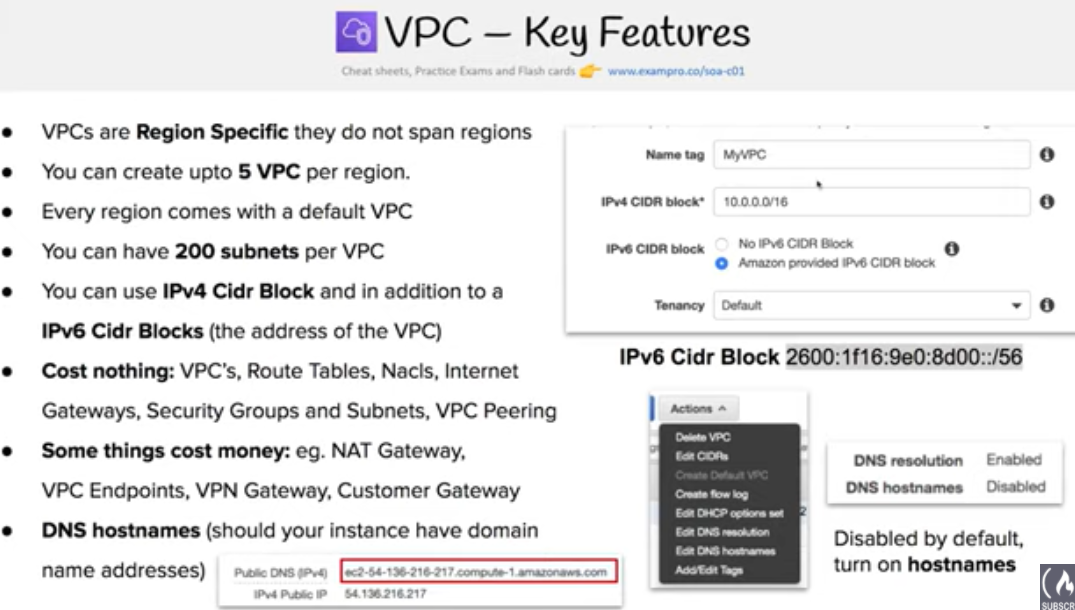
AWS Virtual Private Cloud – VPC

# VPC Overview & Components

* A virtual private cloud (VPC) is a virtual network dedicated to the AWS account. It is logically isolated from other virtual networks in the AWS cloud.
* VPC allows the user to select IP address range, create subnets, and configure route tables, network gateways, and security settings.
* **VPC Sizing**
  + VPC needs a set of IP addresses in the form of a **Classless Inter-Domain Routing (CIDR)** block for e.g, *10.0.0.0/16, which allows 2^16 (65536) IP address to be available*
  + Allowed CIDR block size is between
    - /28 netmask (minimum with 2^4 – 16 available IP address) and
    - /16 netmask (maximum with 2^16 – 65536 IP address)
  + CIDR block from private (non-publicly routable) IP address can be assigned
    - 10.0.0.0 – 10.255.255.255 (10/8 prefix)
    - 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)
    - 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)
  + It’s possible to specify a range of publicly routable IP addresses; however, direct access to the Internet is not currently supported from publicly routable CIDR blocks in a VPC
  + **NOTE** – You can now resize VPC. Read [AWS blog post.](https://aws.amazon.com/about-aws/whats-new/2017/08/amazon-virtual-private-cloud-vpc-now-allows-customers-to-expand-their-existing-vpcs/)
  + Each VPC is separate from any other VPC created with the same CIDR block even if it resides within the same AWS account
* VPC allows [VPC Peering](https://jayendrapatil.com/aws-vpc-peering/) connections with other VPC within the same or different AWS accounts
* Connection between your VPC and corporate or home network can be established, however the CIDR blocks should be not be overlapping for e.g. VPC with CIDR 10.0.0.0/16 can communicate with 10.1.0.0/16 corporate network but the connections would be dropped if it tries to connect to 10.0.37.0/16 corporate network cause of overlapping ip addresses.
* VPC allows you to set tenancy option for the Instances launched in it. By default, the tenancy option is shared. If dedicated option selected, all the instances within it are launched on a dedicated hardware overriding the individual instance tenancy setting
* Deletion of the VPC is possible only after terminating all instances within the VPC, and deleting all the components with the VPC for e.g. subnets, security groups, network ACLs, route tables, Internet gateways, VPC peering connections, and DHCP options





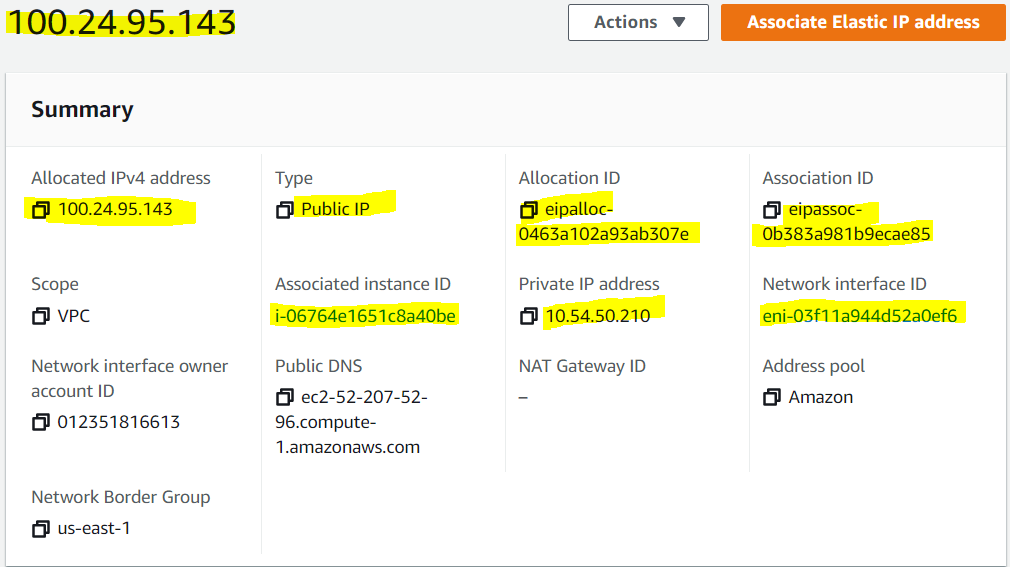
## 

## 

## IP Addresses

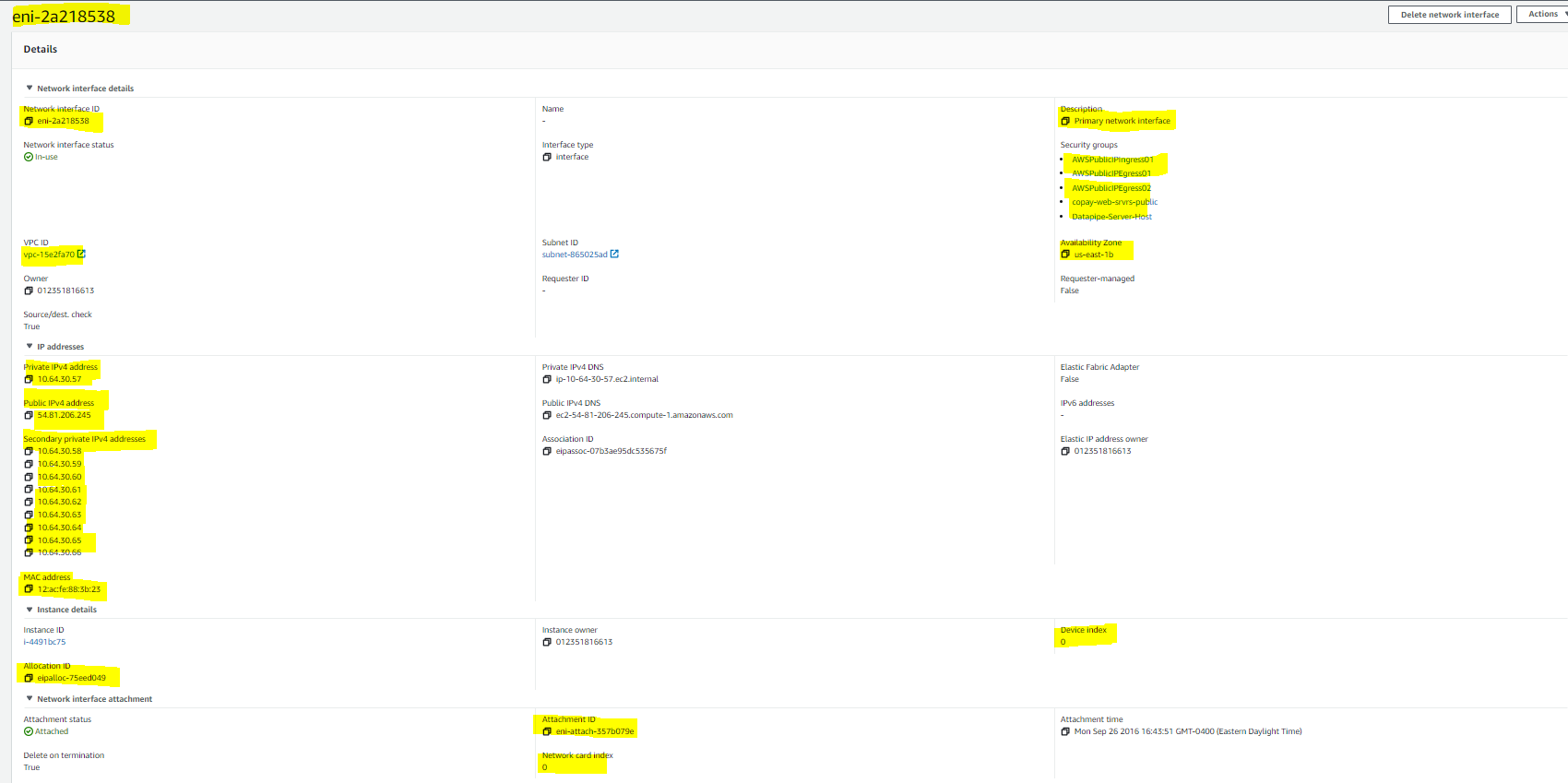
Instances launched in the VPC can have Private, Public and Elastic IP address assigned to it and are properties of ENI (Network Interfaces)

* **Private IP Addresses**
  + **Private IP addresses are not reachable over the Internet, and can be used for communication only between the instances within the VPC**
  + All instances are assigned a private IP address, within the IP address range of the subnet, to the default network interface
  + **Primary IP address is associated with the network interface for its lifetime, even when the instance is stopped and restarted and is released only when the instance is terminated**
  + **Additional Private IP addresses, known as secondary private IP address, can be assigned to the instances and these can be reassigned from one network interface to another**
* **Public IP address**
  + **Public IP addresses are reachable over the Internet, and can be used for communication between instances and the Internet, or with other AWS services that have public endpoints**
  + **Public IP address assignment to the Instance depends if the Public IP Addressing is enabled for the Subnet.**
  + **Public IP address can also be assigned to the Instance by enabling the Public IP addressing during the creation of the instance, which overrides the subnet’s public IP addressing attribute**
  + **Public IP address is assigned from AWS pool of IP addresses and it is not associated with the AWS account and hence is released when the instance is stopped and restarted or terminated.**
* **Elastic IP address**
  + **Elastic IP addresses are static, persistent public IP addresses which can be associated and disassociated with the instance, as required**
  + **Elastic IP address is allocated at an VPC and owned by the account unless released**
  + **A Network Interface can be assigned either a Public IP or an Elastic IP. If you assign an instance, already having an Public IP, an Elastic IP, the public IP is released**
  + **Elastic IP addresses can be moved from one instance to another, which can be within the same or different VPC within the same account**
  + **Elastic IP are charged for non usage i.e. if it is not associated or associated with a stopped instance or an unattached Network Interface**



## Elastic Network Interface (ENI)

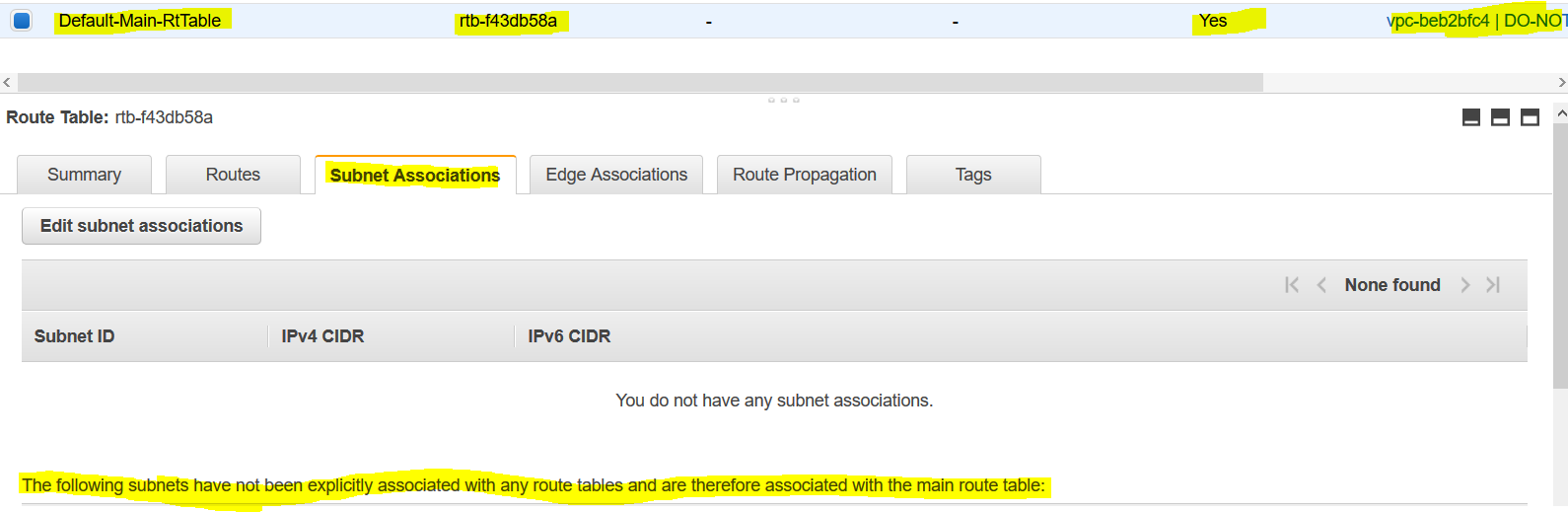
* **Each Instance is attached with default elastic network interface (Primary Network Interface eth0) and cannot be detached from the instance**
* ENI can include the following attributes
  + **Primary private IP address**
  + **One or more secondary private IP addresses**
  + **One Elastic IP address per private IP address**
  + **One public IP address, which can be auto-assigned to the network interface for eth0 when you launch an instance, but only when you create a network interface for eth0 instead of using an existing ENI**
  + **One or more security groups**
  + **A MAC address**
  + **A source/destination check flag**
  + **A description**



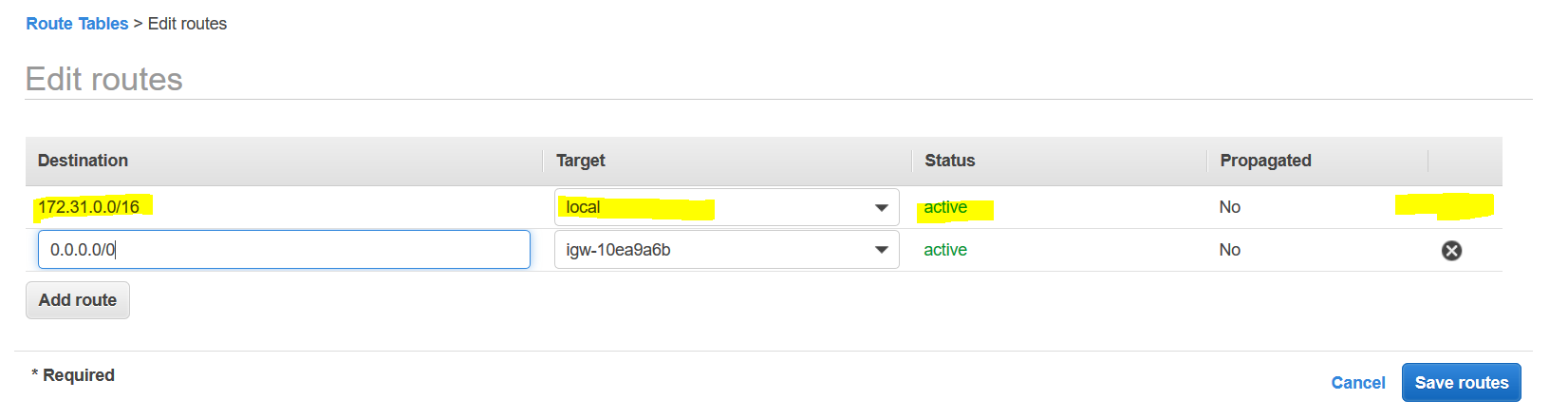
* ENI’s attributes follow the ENI as it is attached or detached from an instance and reattached to another instance. When an ENI is moved from one instance to another, network traffic is redirected to the new instance.
* **Multiple ENIs can be attached to an instance and is useful for use cases:**
  + Create a management network.
  + Use network and security appliances in your VPC.
  + Create dual-homed instances with workloads/roles on distinct subnets.
  + Create a low-budget, high-availability solution.

## Route Tables

* Route table defines rules, termed as routes, which determine where network traffic from the subnet would be routed
* **Each VPC has a implicit router to route network traffic**
* **Each VPC has a Main Route table, and can have multiple custom route tables created**
* **Each Subnet within a VPC must be associated with a single route table at a time**, **while a route table can have multiple subnets associated with it**
* **Subnet, if not explicitly associated to a route table, is implicitly associated with the main route table**



* **Every route table contains a local route that enables communication within a VPC which cannot be modified or deleted.**



* Route priority is decided by matching the most specific route in the route table that matches the traffic
* Route tables needs to be updated to defined routes for Internet gateways, Virtual Private gateways, VPC Peering, VPC Endpoints, NAT Device etc.

## Internet Gateways – IGW

* An Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in the VPC and the Internet.
* IGW imposes no availability risks or bandwidth constraints on the network traffic.
* An Internet gateway serves two purposes:
  + To provide a target in the VPC route tables for Internet-routable traffic,
  + ~~To perform network address translation (NAT) for instances that have been NOT been assigned public IP addresses.~~
* **Enabling Internet access to an Instance requires**
  + Attaching Internet gateway to the VPC
  + Subnet should have route tables associated with the route pointing to the Internet gateway
  + Instances should have a Public IP or Elastic IP address assigned
  + Security groups and NACLs associated with the Instance should allow relevant traffic

## NAT

* NAT device enables instances in a private subnet to connect to the Internet or other AWS services, but prevents the Internet from initiating connections with the instances.
* **NAT devices do not support IPv6 traffic, use an egress-only Internet gateway instead.**

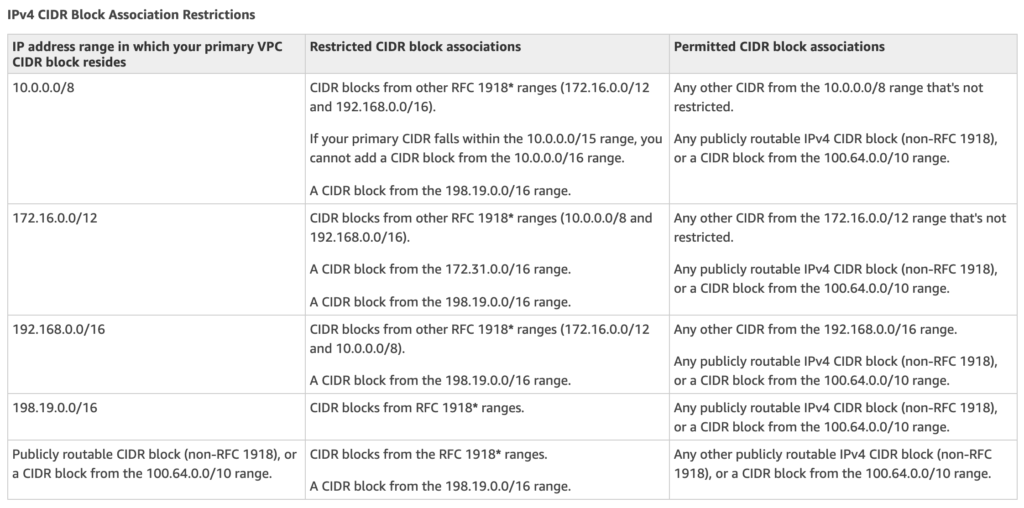
Refer to My Blog Post about [VPC NAT](https://jayendrapatil.com/aws-vpc-nat/)

## Egress-only Internet gateway

* **Egress-only Internet gateway works as a NAT gateway, but for IPv6 traffic**
* Egress-only Internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows outbound communication over IPv6 from instances in the VPC to the Internet, and prevents the Internet from initiating an IPv6 connection with the instances.
* **An egress-only Internet gateway is for use with IPv6 traffic only. To enable outbound-only Internet communication over IPv4, use a NAT gateway instead.**

## VPC & Subnet Sizing

* VPC supports IPv4 and IPv6 addressing, and has different CIDR block size limits for each
* IPv6 CIDR block can be optionally associated with the VPC
* **VPC IPv4 CIDR block cannot be modified once created i.e. cannot increase or decrease the size of an existing CIDR block**.
* However, **secondary CIDR blocks can be associated with the VPC to extend the VPC**
* Limitations
  + **allowed block size is between a /28 netmask and /16 netmask.**
  + **CIDR block must not overlap with any existing CIDR block that’s associated with the VPC.**
  + **CIDR block must not be the same or larger than the CIDR range of a route in any of the VPC route tables for e.g. for a CIDR block 10.0.0.0/24, can only associate smaller CIDR blocks like 10.0.0.0/25**



## VPC Security

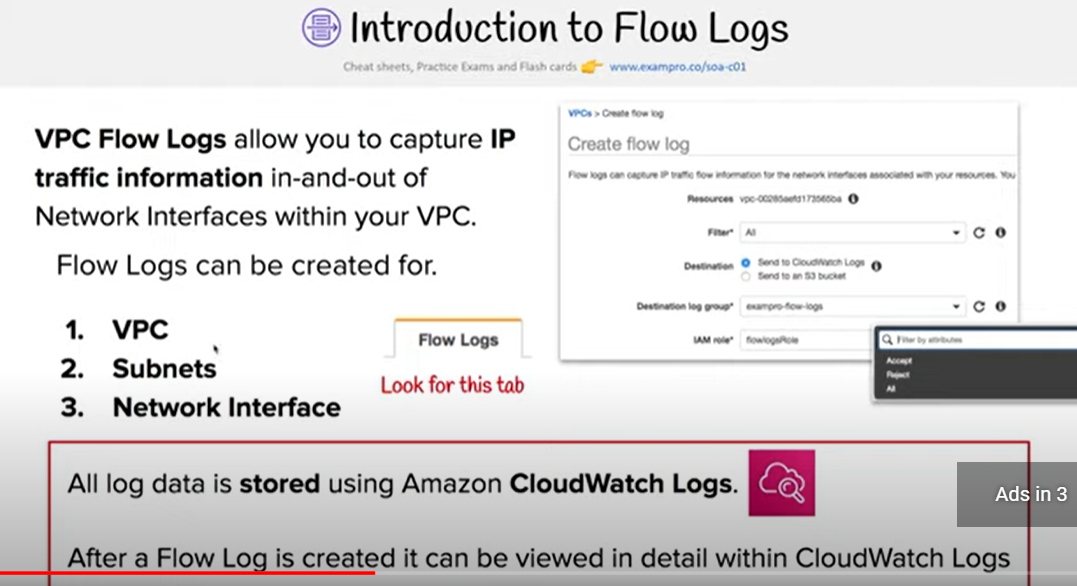
Security within a VPC is provided through

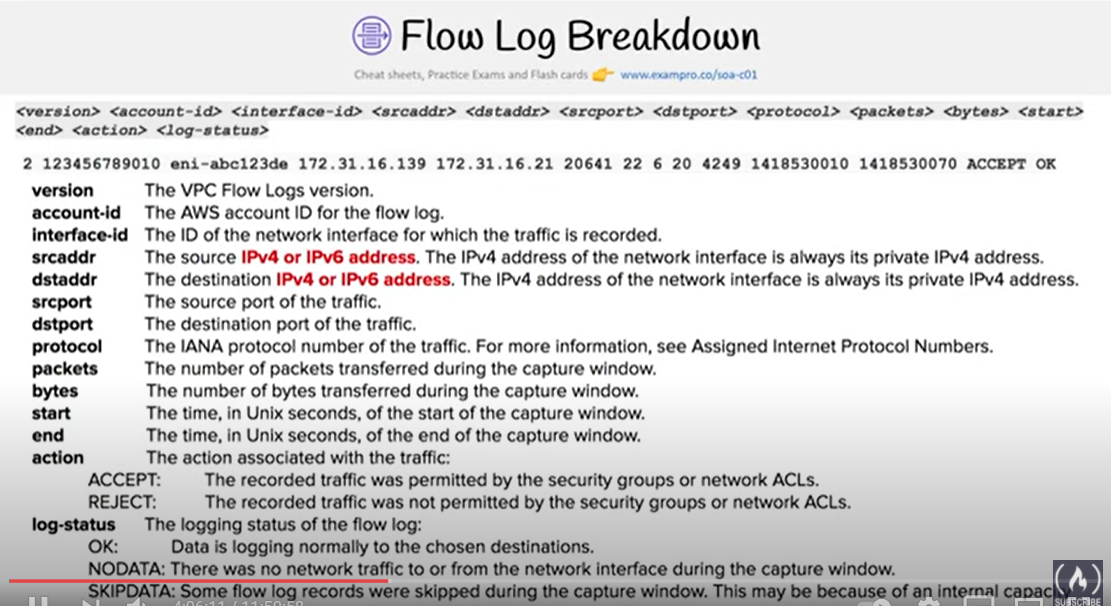
* **Security groups – Act as a firewall for associated EC2 instances, controlling both inbound and outbound traffic at the instance level**
* **Network access control lists (ACLs) – Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level**
* Flow logs – Capture information about the IP traffic going to and from network interfaces in your VPC

### Security Groups & NACLs

Refer to My Blog Post about [AWS Security Group vs NACLs](https://jayendrapatil.com/aws-vpc-security-group-vs-nacls/)

## VPC Flow logs

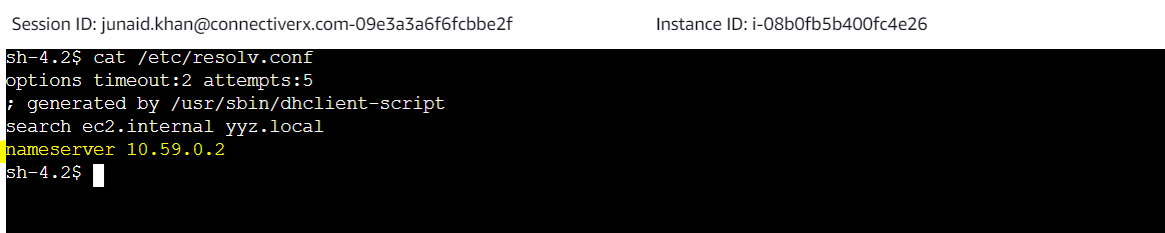




* VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in the VPC and can help in monitoring the traffic or troubleshooting any connectivity issues
* Flow log data is stored using Amazon CloudWatch Logs
* Flow log can be created for the entire VPC, subnets or each network interface. If enabled, for entire VPC or subnet all the network interfaces are monitored
* Flow logs do not capture real-time log streams for network interfaces.
* Flow logs can be created for network interfaces that are created by other AWS services; for example, Elastic Load Balancing, RDS, ElastiCache, Redshift, and WorkSpaces

## Subnets

* **Subnet spans a single Availability Zone, distinct locations engineered to be isolated from failures in other AZs, and cannot span across AZs**
* **Subnet can be configured with an Internet gateway to enable communication over the Internet, or virtual private gateway (VPN) connection to enable communication with your corporate network**
* **Subnet can be Public or Private and it depends on whether it has Internet connectivity i.e. is able to route traffic to the Internet through the IGW**
* **Instances within the Public Subnet should be assigned a Public IP or Elastic IP address to be able to communicate with the Internet**
* For Subnets not connected to the Internet, but has traffic routed through Virtual Private Gateway only is termed as VPN-only subnet
* Subnets can be configured to Enable assignment of the Public IP address to all the Instances launched within the Subnet by default, which can be overridden during the creation of the Instance
* **Subnet Sizing**
  + **CIDR block assigned to the Subnet can be the same as the VPC CIDR, in this case you can launch only one subnet within your VPC**
  + **CIDR block assigned to the Subnet can be a subset of the VPC CIDR, which allows you to launch multiple subnets within the VPC**
  + **CIDR block assigned to the subnet should not be overlapping**
  + **CIDR block size allowed is between**
    - **/28 netmask (minimum with 2^4 – 16 available IP address) and**
    - **/16 netmask (maximum with 2^16 – 65536 IP address)**
  + **AWS reserves 5 IPs address (first 4 and last 1 IP address) in each Subnet which are not available for use and cannot be assigned to an instance. for e.g. for a Subnet with a CIDR block 10.0.0.0/24 the following five IPs are reserved**
    - **10.0.0.0: Network address**
    - **10.0.0.1: Reserved by AWS for the VPC router**
    - **10.0.0.2: Reserved by AWS for mapping to Amazon-provided DNS**



* + - **10.0.0.3: Reserved by AWS for future use**
    - **10.0.0.255: Network broadcast address. AWS does not support broadcast in a VPC, therefore the address is reserved.**
* **Subnet Routing**
  + **Each Subnet is associated with a route table which controls the traffic.**
* **Subnet Security**
  + **Subnet security can be configured using Security groups and NACLs**
  + **Security groups works at instance level, NACLs work at the subnet level**

## Shared VPCs

* VPC sharing allows multiple AWS accounts to create their application resources, such as EC2 instances, RDS databases, Redshift clusters, and AWS Lambda functions, into shared, centrally-managed VPCs.
* In this model, the account that owns the VPC (owner) shares one or more subnets with other accounts (participants) that belong to the same organization from AWS Organizations.
* After a subnet is shared, the participants can view, create, modify, and delete their application resources in the subnets shared with them. Participants cannot view, modify, or delete resources that belong to other participants or the VPC owner.

## VPC Endpoints

Refer to My Blog Post about [VPC Endpoint](https://jayendrapatil.com/aws-vpc-endpoints/)

## VPC Peering

Refer to My Blog Post about [VPC Peering](https://jayendrapatil.com/aws-vpc-peering/)

## VPC VPN Connections & CloudHub

Refer to My Blog Post about [AWS VPC VPN CloudHub Connections](https://jayendrapatil.com/aws-vpc-vpn-cloudhub/)

[do\_widget id=text-15]

## AWS Certification Exam Practice Questions

1. You have a business-to-business web application running in a VPC consisting of an Elastic Load Balancer (ELB), web servers, application servers and a database. Your web application should only accept traffic from predefined customer IP addresses. Which two options meet this security requirement? Choose 2 answers
   1. Configure web server VPC security groups to allow traffic from your customers’ IPs (Web server is behind the ELB and customer IPs will never reach web servers)
   2. **Configure your web servers to filter traffic based on the ELB’s “X-forwarded-for” header** (get the customer IPs and create a custom filter to restrict access. Refer [link](https://aws.amazon.com/premiumsupport/knowledge-center/log-client-ip-load-balancer-apache/))
   3. **Configure ELB security groups to allow traffic from your customers’ IPs and deny all outbound traffic**(ELB will see the customer IPs so can restrict access, deny all is basically have no rules in outbound traffic, implicit, and its stateful so would work)
   4. Configure a VPC NACL to allow web traffic from your customers’ IPs and deny all outbound traffic (NACL is stateless, deny all will not work)
2. A user has created a VPC with public and private subnets using the VPC Wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24. Which of the below mentioned entries are required in the main route table to allow the instances in VPC to communicate with each other?
   1. Destination : 20.0.0.0/24 and Target : VPC
   2. Destination : 20.0.0.0/16 and Target : ALL
   3. Destination : 20.0.0.0/0 and Target : ALL
   4. **Destination : 20.0.0.0/16 and Target : Local**
3. A user has created a VPC with two subnets: one public and one private. The user is planning to run the patch update for the instances in the private subnet. How can the instances in the private subnet connect to the internet?
   1. Use the internet gateway with a private IP
   2. Allow outbound traffic in the security group for port 80 to allow internet updates
   3. The private subnet can never connect to the internet
   4. **Use NAT with an elastic IP**
4. A user has launched an EC2 instance and installed a website with the Apache webserver. The webserver is running but the user is not able to access the website from the Internet. What can be the possible reason for this failure?
   1. **The security group of the instance is not configured properly.**
   2. The instance is not configured with the proper key-pairs.
   3. The Apache website cannot be accessed from the Internet.
   4. Instance is not configured with an elastic IP.
5. A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is true in this scenario?
   1. AWS VPC will automatically create a NAT instance with the micro size
   2. **VPC bounds the main route table with a private subnet and a custom route table with a public subnet**
   3. User has to manually create a NAT instance
   4. VPC bounds the main route table with a public subnet and a custom route table with a private subnet
6. A user has created a VPC with public and private subnets. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.1.0/24 and the public subnet uses CIDR 20.0.0.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group of the NAT instance. Which of the below mentioned entries is not required for the NAT security group?
   1. For Inbound allow Source: 20.0.1.0/24 on port 80
   2. For Outbound allow Destination: 0.0.0.0/0 on port 80
   3. **For Inbound allow Source: 20.0.0.0/24 on port 80**
   4. For Outbound allow Destination: 0.0.0.0/0 on port 443
7. A user has created a VPC with CIDR 20.0.0.0/24. The user has used all the IPs of CIDR and wants to increase the size of the VPC. The user has two subnets: public (20.0.0.0/25) and private (20.0.0.128/25). How can the user change the size of the VPC?
   1. The user can delete all the instances of the subnet. Change the size of the subnets to 20.0.0.0/32 and 20.0.1.0/32, respectively. Then the user can increase the size of the VPC using CLI
   2. **It is not possible to change the size of the VPC once it has been created (NOTE – You can now increase the VPC size. Read**[**Post**](https://aws.amazon.com/about-aws/whats-new/2017/08/amazon-virtual-private-cloud-vpc-now-allows-customers-to-expand-their-existing-vpcs/)**)**
   3. User can add a subnet with a higher range so that it will automatically increase the size of the VPC
   4. User can delete the subnets first and then modify the size of the VPC
8. A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the web server security group (WebSecGrp)?
   1. **Configure Destination as DB Security group ID (DbSecGrp) for port 3306 Outbound**
   2. Configure port 80 for Destination 0.0.0.0/0 Outbound
   3. Configure port 3306 for source 20.0.0.0/24 InBound
   4. Configure port 80 InBound for source 20.0.0.0/16
9. A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 by mistake. The user is trying to create another subnet of CIDR 20.0.0.1/24. How can the user create the second subnet?
   1. There is no need to update the subnet as VPC automatically adjusts the CIDR of the first subnet based on the second subnet’s CIDR
   2. The user can modify the first subnet CIDR from the console
   3. **It is not possible to create a second subnet as one subnet with the same CIDR as the VPC has been created**
   4. The user can modify the first subnet CIDR with AWS CLI
10. A user has setup a VPC with CIDR 20.0.0.0/16. The VPC has a private subnet (20.0.1.0/24) and a public subnet (20.0.0.0/24). The user’s data centre has CIDR of 20.0.54.0/24 and 20.1.0.0/24. If the private subnet wants to communicate with the data centre, what will happen?
    1. It will allow traffic communication on both the CIDRs of the data centre
    2. It will not allow traffic with data centre on CIDR 20.1.0.0/24 but allows traffic communication on 20.0.54.0/24
    3. It will not allow traffic communication on any of the data centre CIDRs
    4. **It will allow traffic with data centre on CIDR 20.1.0.0/24 but does not allow on 20.0.54.0/24**(as the CIDR block would be overlapping)
11. A user has created a VPC with public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The private subnet uses CIDR 20.0.0.0/24 . The NAT instance ID is i-a12345. Which of the below mentioned entries are required in the main route table attached with the private subnet to allow instances to connect with the internet?
    1. **Destination: 0.0.0.0/0 and Target: i-a12345**
    2. Destination: 20.0.0.0/0 and Target: 80
    3. Destination: 20.0.0.0/0 and Target: i-a12345
    4. Destination: 20.0.0.0/24 and Target: i-a12345
12. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user’s data centre. The user’s data centre has CIDR 172.28.0.0/12. The user has also setup a NAT instance (i-123456) to allow traffic to the internet from the VPN subnet. Which of the below mentioned options is not a valid entry for the main route table in this scenario?
    1. **Destination: 20.0.1.0/24 and Target: i-12345**
    2. Destination: 0.0.0.0/0 and Target: i-12345
    3. Destination: 172.28.0.0/12 and Target: vgw-12345
    4. Destination: 20.0.0.0/16 and Target: local
13. A user has created a VPC with CIDR 20.0.0.0/16. The user has created one subnet with CIDR 20.0.0.0/16 in this VPC. The user is trying to create another subnet with the same VPC for CIDR 20.0.0.1/24. What will happen in this scenario?
    1. The VPC will modify the first subnet CIDR automatically to allow the second subnet IP range
    2. It is not possible to create a subnet with the same CIDR as VPC
    3. The second subnet will be created
    4. **It will throw a CIDR overlaps error**
14. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created both Public and VPN-Only subnets along with hardware VPN access to connect to the user’s data centre. The user has not yet launched any instance as well as modified or deleted any setup. He wants to delete this VPC from the console. Will the console allow the user to delete the VPC?
    1. Yes, the console will delete all the setups and also delete the virtual private gateway
    2. No, the console will ask the user to manually detach the virtual private gateway first and then allow deleting the VPC
    3. **Yes, the console will delete all the setups and detach the virtual private gateway**
    4. No, since the NAT instance is running
15. A user has created a VPC with the public and private subnets using the VPC wizard. The VPC has CIDR 20.0.0.0/16. The public subnet uses CIDR 20.0.1.0/24. The user is planning to host a web server in the public subnet (port 80) and a DB server in the private subnet (port 3306). The user is configuring a security group for the public subnet (WebSecGrp) and the private subnet (DBSecGrp). Which of the below mentioned entries is required in the private subnet database security group (DBSecGrp)?
    1. **Allow Inbound on port 3306 for Source Web Server Security Group (WebSecGrp)**
    2. Allow Inbound on port 3306 from source 20.0.0.0/16
    3. Allow Outbound on port 3306 for Destination Web Server Security Group (WebSecGrp.
    4. Allow Outbound on port 80 for Destination NAT Instance IP
16. A user has created a VPC with a subnet and a security group. The user has launched an instance in that subnet and attached a public IP. The user is still unable to connect to the instance. The internet gateway has also been created. What can be the reason for the error?
    1. **The internet gateway is not configured with the route table**
    2. The private IP is not present
    3. The outbound traffic on the security group is disabled
    4. The internet gateway is not configured with the security group
17. A user has created a subnet in VPC and launched an EC2 instance within it. The user has not selected the option to assign the IP address while launching the instance. Which of the below mentioned statements is true with respect to the Instance requiring access to the Internet?
    1. The instance will always have a public DNS attached to the instance by default
    2. The user can directly attach an elastic IP to the instance
    3. The instance will never launch if the public IP is not assigned
    4. **The user would need to create an internet gateway and then attach an elastic IP to the instance to connect from internet**
18. A user has created a VPC with public and private subnets using the VPC wizard. Which of the below mentioned statements is not true in this scenario?
    1. **VPC will create a routing instance and attach it with a public subnet**
    2. VPC will create two subnets
    3. VPC will create one internet gateway and attach it to VPC
    4. VPC will launch one NAT instance with an elastic IP
19. A user has created a VPC with the public subnet. The user has created a security group for that VPC. Which of the below mentioned statements is true when a security group is created?
    1. It can connect to the AWS services, such as S3 and RDS by default
    2. It will have all the inbound traffic by default
    3. **It will have all the outbound traffic by default**
    4. It will by default allow traffic to the internet gateway
20. A user has created a VPC with CIDR 20.0.0.0/16 using VPC Wizard. The user has created a public CIDR (20.0.0.0/24) and a VPN only subnet CIDR (20.0.1.0/24) along with the hardware VPN access to connect to the user’s data centre. Which of the below mentioned components is not present when the VPC is setup with the wizard?
    1. Main route table attached with a VPN only subnet
    2. **A NAT instance configured to allow the VPN subnet instances to connect with the internet**
    3. Custom route table attached with a public subnet
    4. An internet gateway for a public subnet
21. A user has created a VPC with public and private subnets using the VPC wizard. The user has not launched any instance manually and is trying to delete the VPC. What will happen in this scenario?
    1. It will not allow to delete the VPC as it has subnets with route tables
    2. It will not allow to delete the VPC since it has a running route instance
    3. It will terminate the VPC along with all the instances launched by the wizard
    4. **It will not allow to delete the VPC since it has a running NAT instance**
22. A user has created a public subnet with VPC and launched an EC2 instance within it. The user is trying to delete the subnet. What will happen in this scenario?
    1. It will delete the subnet and make the EC2 instance as a part of the default subnet
    2. **It will not allow the user to delete the subnet until the instances are terminated**
    3. It will delete the subnet as well as terminate the instances
    4. Subnet can never be deleted independently, but the user has to delete the VPC first
23. A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25 and a private subnet with CIDR 20.0.0.128/25. The user has launched one instance each in the private and public subnets. Which of the below mentioned options cannot be the correct IP address (private IP) assigned to an instance in the public or private subnet?
    1. **20.0.0.255**
    2. 20.0.0.132
    3. 20.0.0.122
    4. 20.0.0.55
24. A user has created a VPC with CIDR 20.0.0.0/16. The user has created public and VPN only subnets along with hardware VPN access to connect to the user’s datacenter. The user wants to make so that all traffic coming to the public subnet follows the organization’s proxy policy. How can the user make this happen?
    1. Setting up a NAT with the proxy protocol and configure that the public subnet receives traffic from NAT
    2. Setting up a proxy policy in the internet gateway connected with the public subnet
    3. It is not possible to setup the proxy policy for a public subnet
    4. **Setting the route table and security group of the public subnet which receives traffic from a virtual private gateway**
25. A user has created a VPC with CIDR 20.0.0.0/16 using the wizard. The user has created a public subnet CIDR (20.0.0.0/24) and VPN only subnets CIDR (20.0.1.0/24) along with the VPN gateway (vgw-12345) to connect to the user’s data centre. Which of the below mentioned options is a valid entry for the main route table in this scenario?
    1. Destination: 20.0.0.0/24 and Target: vgw-12345
    2. Destination: 20.0.0.0/16 and Target: ALL
    3. Destination: 20.0.1.0/16 and Target: vgw-12345
    4. **Destination: 0.0.0.0/0 and Target: vgw-12345**
26. Which two components provide connectivity with external networks? When attached to an Amazon VPC which two components provide connectivity with external networks? Choose 2 answers
    1. Elastic IPs (EIP) (Does not provide connectivity, public IP address will do as well)
    2. NAT Gateway (NAT) (Not Attached to VPC and still needs IGW)
    3. **Internet Gateway (IGW)**
    4. **Virtual Private Gateway (VGW)**
27. You are attempting to connect to an instance in Amazon VPC without success You have already verified that the VPC has an Internet Gateway (IGW) the instance has an associated Elastic IP (EIP) and correct security group rules are in place. Which VPC component should you evaluate next?
    1. The configuration of a NAT instance
    2. **The configuration of the Routing Table**
    3. The configuration of the internet Gateway (IGW)
    4. The configuration of SRC/DST checking
28. If you want to launch Amazon Elastic Compute Cloud (EC2) Instances and assign each Instance a predetermined private IP address you should:
    1. Assign a group or sequential Elastic IP address to the instances
    2. Launch the instances in a Placement Group
    3. **Launch the instances in the Amazon virtual Private Cloud (VPC)**
    4. Use standard EC2 instances since each instance gets a private Domain Name Service (DNS) already
    5. Launch the Instance from a private Amazon Machine image (AMI)
29. A user has recently started using EC2. The user launched one EC2 instance in the default subnet in EC2-VPC Which of the below mentioned options is not attached or available with the EC2 instance when it is launched?
    1. Public IP address
    2. Internet gateway
    3. **Elastic IP**
    4. Private IP address
30. A user has created a VPC with CIDR 20.0.0.0/24. The user has created a public subnet with CIDR 20.0.0.0/25. The user is trying to create the private subnet with CIDR 20.0.0.128/25. Which of the below mentioned statements is true in this scenario?
    1. It will not allow the user to create the private subnet due to a CIDR overlap
    2. **It will allow the user to create a private subnet with CIDR as 20.0.0.128/25**
    3. This statement is wrong as AWS does not allow CIDR 20.0.0.0/25
    4. It will not allow the user to create a private subnet due to a wrong CIDR range
31. A user has created a VPC with CIDR 20.0.0.0/16 with only a private subnet and VPN connection using the VPC wizard. The user wants to connect to the instance in a private subnet over SSH. How should the user define the security rule for SSH?
    1. **Allow Inbound traffic on port 22 from the user’s network**
    2. The user has to create an instance in EC2 Classic with an elastic IP and configure the security group of a private subnet to allow SSH from that elastic IP
    3. The user can connect to a instance in a private subnet using the NAT instance
    4. Allow Inbound traffic on port 80 and 22 to allow the user to connect to a private subnet over the Internet
32. A company wants to implement their website in a virtual private cloud (VPC). The web tier will use an Auto Scaling group across multiple Availability Zones (AZs). The database will use Multi-AZ RDS MySQL and should not be publicly accessible. What is the minimum number of subnets that need to be configured in the VPC?
    1. 1
    2. 2
    3. 3
    4. **4**(2 public subnets for web instances in multiple AZs and 2 private subnets for RDS Multi-AZ)
33. Which of the following are characteristics of Amazon VPC subnets? Choose 2 answers
    1. **Each subnet maps to a single Availability Zone**
    2. A CIDR block mask of /25 is the smallest range supported
    3. Instances in a private subnet can communicate with the Internet only if they have an Elastic IP.
    4. **By default, all subnets can route between each other, whether they are private or public**
    5. Each subnet spans at least 2 Availability zones to provide a high-availability environment
34. You need to design a VPC for a web-application consisting of an Elastic Load Balancer (ELB). a fleet of web/application servers, and an RDS database The entire Infrastructure must be distributed over 2 availability zones. Which VPC configuration works while assuring the database is not available from the Internet?
    1. One public subnet for ELB one public subnet for the web-servers, and one private subnet for the database
    2. One public subnet for ELB two private subnets for the web-servers, two private subnets for RDS
    3. **Two public subnets for ELB two private subnets for the web-servers and two private subnets for RDS**
    4. Two public subnets for ELB two public subnets for the web-servers, and two public subnets for RDS
35. You have deployed a three-tier web application in a VPC with a CIDR block of 10.0.0.0/28. You initially deploy two web servers, two application servers, two database servers and one NAT instance tor a total of seven EC2 instances. The web, application and database servers are deployed across two availability zones (AZs). You also deploy an ELB in front of the two web servers, and use Route53 for DNS Web traffic gradually increases in the first few days following the deployment, so you attempt to double the number of instances in each tier of the application to handle the new load unfortunately some of these new instances fail to launch. Which of the following could the root caused? (Choose 2 answers) **[PROFESSIONAL]**
    1. The Internet Gateway (IGW) of your VPC has scaled-up adding more instances to handle the traffic spike, reducing the number of available private IP addresses for new instance launches.
    2. AWS reserves one IP address in each subnet’s CIDR block for Route53 so you do not have enough addresses left to launch all of the new EC2 instances.
    3. AWS reserves the first and the last private IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.
    4. **The ELB has scaled-up. Adding more instances to handle the traffic reducing the number of available private IP addresses for new instance launches**
    5. **AWS reserves the first four and the last IP address in each subnet’s CIDR block so you do not have enough addresses left to launch all of the new EC2 instances.**
36. A user wants to access RDS from an EC2 instance using IP addresses. Both RDS and EC2 are in the same region, but different AZs. Which of the below mentioned options help configure that the instance is accessed faster?
    1. **Configure the Private IP of the Instance in RDS security group**(Recommended as the data is transferred within the the Amazon network and not through internet – Refer [link](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_WorkingWithSecurityGroups.html#USER_WorkingWithSecurityGroups.Authorizing%5C))
    2. Security group of EC2 allowed in the RDS security group
    3. Configuring the elastic IP of the instance in RDS security group
    4. Configure the Public IP of the instance in RDS security group
37. In regards to VPC, select the correct statement:
    1. **You can associate multiple subnets with the same Route Table.**
    2. You can associate multiple subnets with the same Route Table, but you can’t associate a subnet with only one Route Table.
    3. You can’t associate multiple subnets with the same Route Table.
    4. None of these.
38. You need to design a VPC for a web-application consisting of an ELB a fleet of web application servers, and an RDS DB. The entire infrastructure must be distributed over 2 AZ. Which VPC configuration works while assuring the DB is not available from the Internet?
    1. One Public Subnet for ELB, one Public Subnet for the web-servers, and one private subnet for the DB
    2. One Public Subnet for ELB, two Private Subnets for the web-servers, and two private subnets for the RDS
    3. **Two Public Subnets for ELB, two private Subnet for the web-servers, and two private subnet for the RDS**
    4. Two Public Subnets for ELB, two Public Subnet for the web-servers, and two public subnets for the RDS
39. You have an Amazon VPC with one private subnet and one public subnet with a Network Address Translator (NAT) server. You are creating a group of Amazon Elastic Cloud Compute (EC2) instances that configure themselves at startup via downloading a bootstrapping script from Amazon Simple Storage Service (S3) that deploys an application via GIT. Which setup provides the highest level of security?
    1. **Amazon EC2 instances in private subnet, no EIPs, route outgoing traffic via the NAT**
    2. Amazon EC2 instances in public subnet, no EIPs, route outgoing traffic via the Internet Gateway (IGW)
    3. Amazon EC2 instances in private subnet, assign EIPs, route outgoing traffic via the Internet Gateway (IGW)
    4. Amazon EC2 instances in public subnet, assign EIPs, route outgoing traffic via the NAT
40. You have launched an Amazon Elastic Compute Cloud (EC2) instance into a public subnet with a primary private IP address assigned, an internet gateway is attached to the VPC, and the public route table is configured to send all Internet-based traffic to the Internet gateway. The instance security group is set to allow all outbound traffic but cannot access the Internet. Why is the Internet unreachable from this instance?
    1. **The instance does not have a public IP address**
    2. The Internet gateway security group must allow all outbound traffic.
    3. The instance security group must allow all inbound traffic.
    4. The instance “Source/Destination check” property must be enabled.
41. You have an environment that consists of a public subnet using Amazon VPC and 3 instances that are running in this subnet. These three instances can successfully communicate with other hosts on the Internet. You launch a fourth instance in the same subnet, using the same AMI and security group configuration you used for the others, but find that this instance cannot be accessed from the internet. What should you do to enable Internet access?
    1. Deploy a NAT instance into the public subnet.
    2. **Assign an Elastic IP address to the fourth instance**
    3. Configure a publically routable IP Address in the host OS of the fourth instance.
    4. Modify the routing table for the public subnet.
42. You have a load balancer configured for VPC, and all back-end Amazon EC2 instances are in service. However, your web browser times out when connecting to the load balancer’s DNS name. Which options are probable causes of this behavior? Choose 2 answers
    1. **The load balancer was not configured to use a public subnet with an Internet gateway configured**
    2. The Amazon EC2 instances do not have a dynamically allocated private IP address
    3. **The security groups or network ACLs are not property configured for web traffic.**
    4. The load balancer is not configured in a private subnet with a NAT instance.
    5. The VPC does not have a VGW configured.
43. When will you incur costs with an Elastic IP address (EIP)?
    1. When an EIP is allocated.
    2. When it is allocated and associated with a running instance.
    3. **When it is allocated and associated with a stopped instance.**
    4. Costs are incurred regardless of whether the EIP is associated with a running instance.
44. A company currently has a VPC with EC2 Instances. A new instance being launched, which will host an application that works on IPv6. You need to ensure that this instance can initiate outgoing traffic to the Internet. At the same time, you need to ensure that no incoming connection can be initiated from the Internet on to the instance. Which of the following would you add to the VPC for this requirement?
    1. A NAT Instance
    2. A NAT Gateway
    3. An Internet Gateway
    4. **An egress-only Internet gateway**