**1. What is the actual definition of the term “VPC”?**

**Answer**: Well, VPC is a private network space within the Amazon cloud that enables you to launch AWS resources. It’s the actual networking layer of Amazon EC2, about which we have already discussed. Each private network you create on the cloud will be logically separated from other virtual networks in the cloud.

Although the structure of VPC looks similar to a standard network that you’d operate in a data centre, a VPC will have the benefits of the scalable infrastructure of AWS. Another major advantage of VPC is that it is fully customizable. You can create subnets, set up route tables, configure network gateways, setup network access control lists, choose IP address range, and many more in a Virtual Private Cloud.

**2. What are the components of Amazon VPC?**

**Answer**: The foremost element in Amazon VPC architecture is VPC network itself. It’s a logically separated part of AWS cloud. It’s possible to define your Virtual Private Cloud’s IP address from the range you’ve chosen. The second element is the Internet Gateway which is the connecting point between your VPC and the public internet. Subnets are the functional parts of your private cloud’s IP address range.

NAT Gateways are used to connect between instances of your private subnet with internet or other AWS services. Customer Gateways are your side of a VPN connection in AWS while Virtual Private Gateways are Amazon VPC side of VPN connection.

**3. What are Internet Gateways in VPC?**

**Answer**: An Internet Gateway is highly available, horizontally scaled VPC component. Gateways establish coherent connections between your Amazon VPC network and the internet. There can be only one gateway associated with each VPC. These are the VPC components that provide NAT (Network Address Translation) for instances which have already assigned public IP addresses. In the case of internet routable traffic, such a gateway provides a target in your VPC route tables.

**4. What is a NAT Device?**

**Answer**: A NAT device in your VPC will enable instances in the private subnet to trigger outbound IPv4 traffic to other AWS services/internet while hindering inbound traffic initiated on the internet. Here when traffic goes out to the internet, IP address gets replaced by NAT device’s address and when the response comes back to the instances, the device translates the address of instances back to the private IP addresses. AWS has two types of NAT devices – NAT instance and NAT gateway. Linux AMIs are configured to run as NAT instances. NAT does not support IPv6 as well.

**5. What is a subnet in VPC?**

**Answer**: According to AWS documentation, subnets are nothing but a range of IP addresses in your VPC. It is possible to launch the resources of AWS into your desired subnet. For resources that need internet access, you can use a public subnet. Whereas for resources that don’t need the internet, a private subnet is sufficient.

The default subnet in your VPC must have the netmask value 20 that can give up to 4096 addresses per subnet. The subnet is always confined within a single availability zone whereas VPC can span across multiple zones.

**6. What is the default VPC? Explain its advantages.**

**Answer**: The questions based on default VPC are among the top AWS VPC interview questions. It’s a logically isolated virtual network that gets created automatically in AWS cloud for an account when the user makes use of Amazon EC2 resources for the first time.

You can alter the components of the default VPC as per your need. There are several advantages of a default VPC. Here, a user can access high-level features such as different IPs, network interfaces without creating a separate VPC or launching instances.

**7. What is ELB (Elastic Load Balancing) and how does it affect VPC?**

**Answer**: As the name implies ELB is a load balancer service for AWS deployments. A load balancer divides the amount of work a computer has to do into more computers and get it done faster. In the same way here ELB distributes incoming application traffic into multiple targets like EC2 instances.

There are 3 types of ELBs to ensure scalability, availability, and security for ensuring your applications as fault tolerant. These are classic, network, and application load balancers. Network and application load balancers can be used in conjunction with VPC and these can route traffics to targets within VPCs.

**8. What do you know about VPC Peering?**

**Answer**: You may be asked about the AWS VPC peering bandwidth in AWS VPC interview. It’s simply the networking connection between two VPs in the same network. It’s possible to create a VPC peering connection between your own VPs or VPC with another AWS account within the same region. It’s not needed for AWS to break the existing VPC infrastructure to enable VPC peering. There is no need of a special hardware for this purpose. It’s not creating a VPN connection or network gateway within the AWS.

The main intention behind such a connection is to facilitate data transfer across multiple VPNs spanning different AWS accounts. This type of peering is a one-to-one relationship wherein transitive connection is not supported. And while talking about AWS VPC peering bandwidth, there are no bandwidth limitations for peering connections as well.

**9. What are the differences between Private, Public & Elastic IP Addresses?**

**Answer**: The questions based on Elastic Network Interfaces are among the most common AWS VPC interview questions.

As the name implies, private IP addresses are IP addresses that aren’t accessible over the internet. If you want to communicate between instances in the same network, private IPs are used. At an instance launching time, a private IP from subnet’s IP address range and a DNS hostname is assigned to eth0 of the instance (default network interface).

A private IP address remains associated with the network interface will get released only when the instance is terminated (not when the instance is stopped or restarted). On the contrary, a public IP address is easily accessible over the internet.

When you launch a VPC instance, one public IP will automatically assign to the instance which isn’t associated with your AWS account. Every time you restart and stop the instance, AWS will allocate a new public IP to the instance. The main difference between a public and elastic IP is that elastic IP is persistent. It’ll be associated with your AWS account until you terminate it. Anyhow, you can detach elastic IP from one instance and attach the same IP to a different instance. Elastic IP is also accessible over the internet.

**10. Is there any limit to the number of VPCs, subnets, gateways, VPNs that I can create?**

**Answer**: Yes, there is definitely a limit. You can create 5 VPCs per region. If you want to increase this limit, you’ve to increase the number of internet gateways by the same number. And, per VPC 200 subnets are allowed. 5 elastic IP addresses are allowed per region. The number of Internet, VPN and NAT gateways per region is also set to 5.

**11. Can you illustrate what is CIDR Routing in VPC?**

**Answer**: The questions based on IP address are the common among frequently-asked AWS VPC interview questions. This CIDR question can be answered in the following manner. Classless inter-domain routing (CIDR) is a set of Internet protocol (IP) standards that are used to allocate IP addresses for networks and individual devices.

Generally, A CIDR IP looks like a normal IP address except there is a slash followed by a number in CIDR. This part is called the IP network prefix. In VPC, CIDR block size can be from /16 to /28 in case of IPv4. When you’re creating a VPC, you actually have to specify a range of IP address in form of CIDR just like 10.0.0.0/16. This CIDR is the primary CIDR block of your VPC.

CIDR offers the benefits of effective management of available IP address space and reduce the number of routing table entries.

**12. What are Security Groups in VPC?**

**Answer**: In VPC, a security group’s function is to manage the traffic for the instances. Instances can be single in number or many. Actually, it does act as a virtual firewall that can control inbound and outbound traffic for different EC2 instances. You can manually add rules to each security group to control the traffic within the associated instances.

In AWS console, security groups can be located in both VPC and EC2 sections. By default, all security groups allow outbound traffic. In the same way, you can define rules to allow inbound traffic. But one thing- you are only allowed to create “allow” rules rather setting up denial rules to restrict security permissions. Also, it’s possible to change the rules of a security group irrespective of the time and the process of changing rules will take place instantly.

**13. What do you mean by Network ACLs (Access Control List) in VPC?**

**Answer**: Network ACLs does the similar function of a network security group in VPC; IE controlling inbound and outbound traffic in VPC. The main difference between a network ACL and a security group is that the security group’s role is to act as a firewall for associated EC2 instances whereas an ACL’s role is to serve firewall job for associated subnets. Your VPC generates an ACL automatically by default and it’s modifiable. Unlike a security group, this default network ACL allows all inbound and outbound traffic by default. And it’s possible to associate an ACL with multiple subnets. But at a time, only one subnet can be associated with a network ACL.

You can also create your own custom ACL and it can be associated with a subnet. Such an ACL denies all types of inbound/outbound traffic until you add rules to it.

**14. What is stateful and stateless filtering?**

**Answer**: A stateful filtering checks the origin of the request and triggers automatic replay to the originating computer. On the other hand, stateless filtering only examines the source and destination IPs ignoring whether it’s a new request or replay to a request.

In VPC, security groups carry out stateful filtering whereas network ACLs perform stateless filtering.

**15. What are the functions of an Amazon VPC router?**

**Answer**: VPC router allows Amazon EC2 instances within subnets to interact with Amazon EC2 instances in other subnets within the same VPC. Virtual private gateways, subnets and Internet gateways, etc. can also communicate with each other by means of a VPC router.

**16. How much Amazon charge you for sharing their cloud space with you?**

**Answer**: Basically, for a VPN connection to your VPC, Amazon charges nearly $0.5 for an hour. There is an option to terminate your VPN connection through AWS consoled if you don’t want to charge for this.

AWS internet gateway pricing charges vary through different geographic locations. You’ll be charged from $0.045 up to $0.054 per gateway-hour and GBs of data processed based on your location.

**17. What is PrivateLink from AWS?**

**Answer**: PrivateLink provides utmost availability and scalability for AWS customers to access their services maintaining the traffic within the AWS network. It delivers private connections between VPCs, on-premises applications, etc. securely on Amazon network.

**18. What is ClassicLink in VPC?**

**Answer**: If you want to connect Amazon EC2-classic instances to VPC, you have to use ClassicLink. This work only within the same region and this makes use of private IP addresses. Its working is simple- you just have to enable ClassicLink in your VPC account and associate a security group from VPC to EC2-classic instance.

**19. What is so special about VPC that stands out it from other private clouds?**

**Answer**: There’s no need for a particular hardware, physical data centres or virtual private networks if you want a private network within the cloud – AWS VPC will provide it. The advanced security features of VPC makes it almost invulnerable to privacy & security threats.

**20. What is a VPS?**

**Answer**: Beginners who were trying AWS VPC interview questions for the first time used to get confused with this question, since these terms look similar.

Actually, VPS or Virtual Private Server is none other than the host server offered by web hosting companies like Bluehost and GoDaddy (These companies also provide shared hosting services wherein the server is shared by several users). Here, a single host divided to multiple virtual units, each having an independent function. Each of these units is virtual private servers which can work without depending on one another. You’ll get access to the complete physical server including root access.

In the case of VPC, its functions are similar to that of a VPS but its servers don’t have to place in a single location.

**21. What IP addresses range can be used in a VPC?**

**Answer**: You can use any IPv4 address range, including RFC 1918 or publicly routable IP ranges, for the primary CIDR block. For the secondary CIDR blocks, certain restrictions apply. Publicly routable IP blocks are only reachable via the Virtual Private Gateway and cannot be accessed over the Internet through the Internet gateway. AWS does not advertise customer-owned IP address blocks to the Internet. You can allocate an Amazon-provided IPv6 CIDR block to a VPC by calling the relevant API or via the AWS Management Console.

**22. How to connect My VPC to the Internet?**

**Answer**: It is good news that Amazon VPC enables the creation of an Internet gateway. This allows Amazon EC2 occurrences in the VPC to access the Internet directly. There are numerous connectivity options for my VPC. You can connect your Virtual Private Cloud to the following:

Your corporate data centre with the help of a Hardware Virtual Private Network connection

The Internet through an internet gateway

The Internet as well as your corporate data centre, together. You can do this by using both, the virtual private gateway and the Internet gateway.

**23. What are the elements of Amazon Virtual Private Cloud?**

**Answer**: The Amazon VPC contains various elements:

VPC- a logically secluded virtual network in the Amazon Web Services cloud. You only need to define a Virtual Private Cloud’s IP address space from the range that you select

Internet Gateway- Internet Gateway is the Amazon VPC’s side of a connection to the public internet

Subnet- Subnet is a part of cloud’s IP address space from the range that you select

NAT Gateway- A highly available and managed NAT service for your resources in a private subnet to use the internet

Virtual Private Gateway- This is the Amazon VPC’s side of a VPN connection

Customer Gateway- It is the user’s side of a VPN connection

Router- Routers interconnect subnets and the direct traffic between Virtual Private Gateways, Internet Gateways, NAT gateways as well as subnets.

**24. What are the advantages of using Amazon Web Services VPC?**

**Answer**: It helps you to build a virtual network in the Amazon Web Services cloud. Also, for this process, no hardware, physical data centres or even VPNs will be required. You have absolute power over your own network space. You can control how your network and Amazon EC2 that resources inside your network is actually exposed to the Internet. You also have the leverage to hugely enhance the security options in Amazon VPC to provide more granular access to and from the Amazon EC2 instances in your virtual network.

**25. Can the network traffic in your VPC be monitored?**

**Answer**: Yes, you can use the Amazon VPC flow logs feature to monitor the traffic of network in your Virtual Private Cloud.

**26. Within which Amazon EC2 Region is Amazon VPC available?**

**Answer**: It is available in all Amazon EC2 regions.

**27. Can a VPC span multiple availability zones?**

Answer: Yes, a virtual private cloud can easily span multiple availability zones.

**28. How can you differentiate between stateful and stateless filtering?**

**Answer**: In case of stateful filtering, the point of origination of request is tracked and the reply is sent automatically to the request, which is then returned to the computer from where it originated.

In case of Stateless Filtering, it doesn’t matter whether a new request is generated or an automatic reply is sent to a request, the filter only seeks the origin or destination IP address & port.

**29. How do you specify which availability zone my Amazon EC2 instances are launched in?**

**Answer**: When Amazon EC2 instance is launched you must specify the subnet in which to launch the instance. This instance will be then launched in the availability zone that is associated with the given subnet.

**30. Are there any bandwidth limitations for Internet gateways?**

**Answer**: An Internet gateway is horizontally scaled, highly available as well as redundant. Thus, there are no bandwidth limitations for Internet gateways.

**31. How do you secure Amazon EC2 instances running within My VPC?**

**Answer**: Amazon EC2 security groups are helpful to secure instances within an Amazon VPC. Security groups in VPC help you to specify both inbound as well as outbound network traffic that is allowed to and from each Amazon EC2 instance. The traffic that is not explicitly allowed to or from an instance is automatically denied.

**32. How do you determine which availability zone my subnets are located in?**

**Answer**: In the VPC dashboard, we need to open the desired subnet by clicking on the subnet id and in the details section we can see the name and id of availability zone which subnet belongs to.

**33. What do you understand by default VPC?**

**Answer**: When a user avails Amazon EC2 resources for the first time, a logically isolated virtual network is created automatically in the AWS cloud for the AWS account. In a case where an instance is launched without a subnet ID, it shall automatically be launched in the default VPC.

**34. State the advantage of a default VPC?**

**Answer**: There are several advantages of default VPC. Firstly, if a resource is launched in default VPC, the user can avail the high-end network functions of Amazon VPC along with ease to use Amazon EC2.

Secondly, without creating a VPC or launching the instances, the user can still avail several features such as different IP address, altering the security group membership, egress filtering of the security group and several network interfaces.

**35. How will you differentiate between VPC security groups and VPC network ACLs?**

**Answer**: When we talk about the VPC security group, it is responsible for tracking only the allowed traffic in EC2 instance, which comes in and goes out from Amazon. VPC network ACLs is a lot different. They are responsible for tracking the traffic at the subnet level i.e., the traffic coming in or going out of subnet.