1) You are the AWS architect at YCDIT2, Inc. Your client has a VPC with public and private subnets is created by the VPC wizard. The VPC CIDR is 10.0.0.0/16. The public subnet is 10.0.1.0/24. The architecture you put together includes deploying a web server in the public subnet, receiving HTTP traffic on port 80; it also includes a Database server tier in the private subnet receiving traffic on port 3306. The client SysOps is configuring a security group for the public subnet called WebSG, and the private subnet's security group called DbSG.

Which of the below entries is required in the web server security group?

a) Destination: DB Security group ID (DbSG), Port: 3306, Direction: Outbound
b) Destination: 0.0.0.0/0, Port: 80, Direction: Outbound
c) Source 10.0.1.0/24, Port: 3306, Direction: Inbound
d) Source 10.0.0.0/16, Port: 80, Direction: Inbound

2) Which of the below statements is true for any VPC security group, by default, when it is created?

a) All inbound traffic rule will be explicitly denied
b) All inbound traffic is allowed by default
c) All outbound traffic is allowed by default
d) Traffic to the internet gateway is allowed by default

3) You are the AWS SME at YCDIT2, Inc. You created a VPC with both public and private subnets. The VPC has the CIDR 10.0.0.0/16. The private subnet is 10.0.1.0/24 and the public subnet is 10.0.0.0/24. The goal is to host a web server in the public subnet receiving traffic on port 80, and a DB server in the private subnet receiving traffic on port 3306. The database servers will require in-frequent Internet access for patching and updates. When you are configuring the security group of the NAT instance (NATSG), which of the below mentioned entries is not required?

a) Allow Source: 10.0.1.0/24, Direction: Inbound, Port: 80
b) Allow Destination: 0.0.0.0/0, Direction: Outbound, Port: 80
c) Allow Source: 10.0.0.0/24, Direction: Inbound, Port: 80
d) Allow Destination: 0.0.0.0/0, Direction: Outbound, Port: 443

4) You are the AWS architect at YCDIT2, Inc. You have been tasked to design and launch an EC2 NAT instance in a public subnet in your client's VPC. After creating and successfully testing the NAT Instance. You have also updated you private subnet's route table such that the NAT device is the target for traffic destined to the Internet. However, the private subnet EC2 instances are still not able to connect to the Internet for updates and patch download.
Which of the following steps could be a possible reason for this problem?

a) NAT instance is launched with only one ENI in the public subnet
b) The NAT instance has not been configured with the proper NAT rules to process the private instance's traffic intended for the internet
c) The NAT instance will not work, you need to configure static, one-to-one NAT on the VPC Internet Gateway for private subnet's instances to connect to the Internet
d) Disabling the Source/Destination Check attribute on the NAT instance

5) At which EC2 instance states can the source/destination check attribute be changed? (Choose two)
a) When the NAT instance state is terminated
b) When the NAT instance state is pending
c) When the NAT instance state is running
d) When the NAT instance state is stopped

6) Using the VPC wizard, you have created a VPC with CIDR 10.0.0.0/16 with a VPN-only private subnet and Hardware VPN Access connection. You need to connect to an instance in the private subnet over SSH.
How should you define the instance's security group rule to allow SSH?

a) Allow Inbound traffic for SSH (port 22) from the corporate network
b) Allow port 22 on the security group of the VPN-only subnet to allow SSH inbound
c) Create a public subnet, Implement a NAT instance and use it to connect to the VPN-only subnet instances
d) Allow Inbound traffic on port 22 to allow you to connect to a private subnet over the Internet

7) You have created a VPC with CIDR 10.0.0.0/24. The VPC has two subnets: public (10.0.0.0/25) and private (10.0.0.128/25). For an anticipated project you want to increase the CIDR range your VPC CIDR block, How can you do this?
a) Change the subnet sizes to /28 subnets, then you will have more room to grow your VPC CIDR
b) You can always change a VPC's original CIDR block as needed
c) You can add additional VPC CIDR blocks, but can't change the existing one
d) Delete all the subnets first, only then you can modify the size of the VPC

8) After creating a VPC with CIDR 10.0.0.0/16. with the lack of proper architecture, The AWS SysOps admin created one large subnet of CIDR 10.0.0.0/16. later on, another subnet was needed to host another tier of an application being deployed. The admin is trying to create another subnet of CIDR 10.0.1.0/24.
Can she create the second subnet without disrupting services to the first subnet?

a) Yes, she can configure the new subnet, and AWS will automatically adjust the VPC subnets so both can exist.
b) Yes, Edit the fist subnet from the console to make room for the second one
c) No, It is not possible to create a second subnet as the intended one overlaps with the existing one
d) Yes, Delete the VPC and create a new one

9) You are the AWS SME at YCDIT2, Inc. Your AWS SysOps administrator created a VPC with a public subnet. He created and attached an Internet Gateway to the VPC, and launched an EC2 instance with a public IP in the subnet. He also created a security group for the EC2 instance. When trying to connect to the EC2 instance from the Internet, he was not able to. From the statements below, which could be a possible reason for his inability to connect? (Choose 2)

a) There is no entry in the route table pointing to the internet gateway as a Target
b) The admin did not configure the security group after he created it
c) The security group is denying any outbound traffic to the Internet
d) The admin forgot to create a NACL for the EC2 instance

10) You created a subnet in a custom VPC and launched an EC2 instance in that subnet. During the EC2 instance creation, using AWS console, you did not choose the option to assign a public IP address to your instance. This instance now needs access to the Internet, but it has no public IP address.
How would you solve this internet connectivity issue for this EC2 instance?

a) The instance will always have a public DNS attached to the instance by default
b) Allocate and attach an Elastic IP directly to the instance
c) The instance would not launch if the public IP is not assigned
d) Create an internet gateway, attach it to the VPC, do the needed route table configuration for a public subnet. Adjust security group, and N ACLs configurations to facilitate this, and finally, attach an elastic IP to the instance to connect to the Internet

11) You are the AWS Architect at YCDIT2, Inc. Your client plans to connect their Data Center to their AWS VPC in preparation for an application launch in few months. The application they are launching is chatty and has components in AWS and in the data center, and will be hosted in private AWS subnets in their AWS VPC. It also requires bandwidth and latency guarantees at all times. The solution has to be fault tolerant. Which connectivity method would you recommend for them?

a) One VPN connection with two tunnels between one Customer Gateway and one VGW router on AWS side
b) Two Public VIFs over two Direct connect connections. From two Customer routers to two different DX routers
c) Two Direct connect connections using two Customer routers and two private VIFs to two different Direct connect routers
d) One direct connect connection with one private VIF, and a backup VPN connection from two customer routers

12) You are the architect at YCDIT2, Inc. Your client has a multi AZ infrastructure on AWS, and plans , in few months, to have a centralized, custom, dashboard in the client's data center. The dashboard will need to interact with the multi AZ infrastructure. Data from the Multi AZ will be pulled from the data center. Latency and performance (bandwidth) are key. The solution needs to be up and running within few months.
How would you architect the solution?

a) Use redundant VPN connections to two VGW routers in the region, this should give you access to the infrastructure in all AZs
b) Use direct connect connection to the client VPC, as this will provide access to all AZs in the region, and will also provide better bandwidth and lower latency
c) Use one direct connect connection from the data center to each AZ in the region
d) You can not interact with multiple AZs from one location

13) Using AWS direct connection, with public and private VIFs you can: (Choose 3)

a) Connect to AWS services over the private VIF
b) Connect to your private VPC subnets over the public VIF
c) Connect to your private VPC subnets over the private VIF, and to Public AWS services over the public VIF
d) Substitute your internet connection at your DC with AWS's public Internet through the use of a NAT gateway in your VPC
e) Once connected to your VPC through Direct connect you can connect to all AZs within the region
f) Using IPSec VPN you can connect over the public VIF to remote AWS regions as well

14) Your company has peered two VPCs in the same region, VPC-A and VPC-B. Moreover, your company's HQ is connected to VPC-A using a VPN connection. You want to make this setup more fault tolerant, and ensure that company HQ has connectivity to VPC-A at all times.
How can you architect this solution quickly and cost effectively?

a) Peer the corporate network to VPC-B
b) Connect Corporate network to VPC-B by a VPN connection such that it has another path to VPC-A
c) Configure a second VPN connection between HQ and VPC-A from another customer gateway at the HQ
d) Configure a second VPC peering between VPC-A and VPC-B

15) Your company has seven offices including HQ. The company just implemented an application on AWS in a VPC. The application will be accessed by company employees from all seven locations. Latency and performance are not a big concern, however, the solution needs to be fast, easy to deploy, and cost effective.
How would you architect the solution?

a) Deploy an OpenSSL server on an EC2 instance in your VPC. Have the employees establish SSL based remote access when they need to access the application
b) Establish a site-to-site IPSec VPN from each location to the VPC's VGW and adjust routing to allow access to the application
c) Establish a Direct Connect connection from each location to the VPC
d) You can not connect multiple locations concurrently to your AWS VPC

16) Your company just implemented an HR application on AWS in a VPC. The application will provide payroll and benefits information to the employees and needs to be accessed from all twenty Company locations. Latency and performance are not a big concern, however, the solution needs to be fast and easy to deploy and cost effective. Your solutions should also allow the twenty locations to communicate with one another.
How would you architect the solution?

a) Deploy an OpenSSL server on an EC2 instance in your VPC. Have the employees establish SSL based remote access when they need to access the HR application
b) Establish a site-to-site IPSec VPN from each location to the VPC's VGW and adjust routing to allow access to the application
c) You can not connect multiple locations concurrently to your AWS VPC
d) You need to contact AWS first to increase the 10 VPNs per VGW limit, then configure VPN Cloudhub to connect the 20 locations

17) You are the AWS SME at YCDIT2, Inc. One of the AWS administrators created a VPC with CIDR 10.0.0.0/16, a public and VPN-only subnets with hardware VPN access using the VPC wizard. She has just created the VPC and did not launch any instances, nor has she modified anything after the VPC was launched. Now she wants to delete this VPC using the AWS console.
How can she achieve this?

a) The console will delete the VPC, its components including the Virtual Private Gateway
b) The console will request detaching the Virtual Private Gateway first, then would allow deleting the VPC
c) The console will delete the VPC, its components, and will also detach the Virtual Private Gateway
d) She can't since the NAT instance is running

18) You used the VPC wizard to create a VPC with public and private subnets. The VPC CIDR is 10.0.0.0/16, and the the private subnet CIDR is 10.0.0.0/24.
Which of the below main route table entries is required to allow the instances in the VPC to communicate with one another?

a) Destination : 10.0.0.0/24 and Target : VPC
b) Destination : 10.0.0.0/16 and Target : ALL
c) Destination : 10.0.0.0/0 and Target : ALL
d) Destination : 10.0.0.0/16 and Target : Local

19) When using the VPC wizard to create a VPC with private and public subnets, which of the below statements stands correct? (Choose two)

a) AWS VPC will automatically create a NAT instance with the micro size
b) VPC bounds the main route table with a private subnet and a custom route table with a public subnet
c) User has to select a NAT instance instead of the NAT gateway if needed during the wizard configuration
d) VPC bounds the main route table with a public subnet and a custom route table with a private subnet

20) Your company just partnered with an online training provider. You got assigned the task to architect the solution. The online training provider requested, for security reasons, that any traffic originated from your company's AWS environment and destined to the online provider, be sourced from a maximum of one or two fixed public IP addresses. Your AWS application instances, that should originate this traffic, are behind an ELB. Auto Scaling is also used to increase the application layer instances from 2 to 8 depending on the traffic load received from the ELB. The solution must be highly available.
How would you architect the required solution?

a) Assign two EC2 instances fixed public IPs, force the other instances to send their online provider traffic to these two instances all the time.
b) Configure two NAT instances, one per AZ. Allocate and attach Elastic IP addresses to these instances, route the application EC2 instances traffic destined to the online provider through these two NAT instances, and provide the two Elastic IP addresses to your provider as the fixed source public IPs
c) Use Elastic IPs on the VPC Internet Gateway Public IP since all Internet Traffic passes through them
d) Use the ELB public IP addresses as the first IP addresses required

21) You have three separate VPCs in your AWS account in one region, currently the VPCs are operating separately. However, a new file sharing solution is launched in VPC-1 and you want the other two VPCs, VPC-2, and VPC-3 resources to be able to upload and download files from this file sharing solution.
How can you architect a solution to allow the three VPCs to share the file sharing solution? Taking into account cost effectiveness and speed of deployment.

a) Establish two peering connections between VPC-1 and VPC-2, and VPC-2 and VPC-3
b) Establish a peering connection between VPC-1 and VPC-2, and another between VPC-1 and VPC-3
c) Move the file sharing solution to your data center, and deploy VPN connections from each VPC to the data center
d) You can not share resources between VPCs in AWS

22) Your company has entered an agreement with two other vendors to jointly sell each other's line of products. All three are using VPCs in AWS in the same region. Agreement is , each of the three companies can directly access stock and pricing information of this line of products from the other VPCs. The EC2 instances hosting stock and pricing information in the the three VPCs' are on non-overlapping IP subnets.
How can you architect this solution quickly and cost effectively?

a) Implement an AWS direct connection in a full mesh between the three VPCs
b) Use one of the three company VPCs as a hub and implement a VPN Cloud hub using VPN connections from the other two VPCs
c) Create a full mesh VPC peering connections between the three VPCs and adjust your routing tables to enable traffic flow between them
d) These are different AWS accounts and you can not create VPC peering between them

23) 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 required number of VPC subnets to achieve this?

a) 1
b) 2
c) 3
d) 4

24) You are trying, unsuccessfully, to connect to the EC2 instance you just created in your AWS VPC environment. As part of your troubleshooting effort to fix this, you verified that the VPC has an Internet Gateway (IGW) attached to it, and that the instance has an associated Elastic IP (EIP), and the correct security group rules are in place.
Which other VPC components should you evaluate? (Choose two)

a) The configuration of a NAT instance
b) The configuration of the Route Table
c) The configuration of the internet Gateway (IGW)
d) The configuration of SRC/DST checking
e) The EC2 Instance subnet's N. ACL configuration

25) A data processing application in AWS must pull data from an Internet service. A Solutions Architect is to design a highly available solution to access this data without placing bandwidth constraints on the application traffic.

Which solution meets these requirements?

a) Launch a NAT gateway and add routes for 0.0.0.0/0

b) Attach a VPC endpoint and add routes for 0.0.0.0/0

c) Attach an Internet gateway and add routes for 0.0.0.0/0

d) Deploy NAT instances in a public subnet and add routes for 0.0.0.0/0