**Review Questions**

1. What is the minimum size subnet that you can have in an Amazon VPC?

A. /24

B. /26

C. /28

D. /30

2. You are a solutions architect working for a large travel company that is migrating its existing server estate to AWS. You have recommended that they use a custom Amazon VPC, and they have agreed to proceed. They will need a public subnet for their web servers and a private subnet in which to place their databases. They also require that the web servers and database servers be highly available and that there be a minimum of two web servers and two database servers each. How many subnets should you have to maintain high availability?

A. 2

B. 3

C. 4

D. 1

3. Which of the following is an optional security control that can be applied at the subnet layer of a VPC?

A. Network ACL

B. Security Group

C. Firewall

D. Web application firewall

4. What is the maximum size IP address range that you can have in an Amazon VPC?

A. /16

B. /24

C. /28

D. /30

5. You create a new subnet and then add a route to your route table that routes traffic out from that subnet to the Internet using an IGW. What type of subnet have you created?

A. An internal subnet

B. A private subnet

C. An external subnet

D. A public subnet

6. What happens when you create a new Amazon VPC?

A. A main route table is created by default.

B. Three subnets are created by default— one for each Availability Zone.

C. Three subnets are created by default in one Availability Zone.

D. An IGW is created by default.

7. You create a new VPC in US-East-1 and provision three subnets inside this Amazon VPC. Which of the following statements is true?

A. By default, these subnets will not be able to communicate with each other; you will need to create routes.

B. All subnets are public by default.

C. All subnets will be able to communicate with each other by default.

D. Each subnet will have identical CIDR blocks.

8. How many IGWs can you attach to an Amazon VPC at any one time?

A. 1

B. 2

C. 3

D. 4

9. What aspect of an Amazon VPC is stateful?

Network ACLs

Security groups

Amazon DynamoDB

Amazon S3

10. You have created a custom Amazon VPC with both private and public subnets. You have created a NAT instance and deployed this instance to a public subnet. You have attached an EIP address and added your NAT to the route table. Unfortunately, instances in your private subnet still cannot access the Internet. What may be the cause of this?

A. Your NAT is in a public subnet, but it needs to be in a private subnet.

B. Your NAT should be behind an Elastic Load Balancer.

C. You should disable source/ destination checks on the NAT.

D. Your NAT has been deployed on a Windows instance, but your other instances are Linux. You should redeploy the NAT onto a Linux instance.

11. Which of the following will occur when an Amazon Elastic Block Store (Amazon EBS)-backed Amazon EC2 instance in an Amazon VPC with an associated EIP is stopped and started? (Choose 2 answers)

A. The EIP will be dissociated from the instance.

B. All data on instance-store devices will be lost.

C. All data on Amazon EBS devices will be lost. The ENI is detached.

D. The ENI is detached.

E. The underlying host for the instance is changed.

12. How many VPC Peering connections are required for four VPCs located within the same AWS region to be able to send traffic to each of the others?

A. 3

B. 4

C. 5

D. 6

13. Which of the following AWS resources would you use in order for an EC2-VPC instance to resolve DNS names outside of AWS?

A. A VPC peering connection

B. A DHCP option set

C. A routing rule

D. An IGW

14. Which of the following is the Amazon side of an Amazon VPN connection?

A. An EIP

B. A CGW

C. An IGW

D. A VPG

15. What is the default limit for the number of Amazon VPCs that a customer may have in a region?

A. 5

B. 6

C. 7

D. There is no default maximum number of VPCs within a region.

16. You are responsible for your company’s AWS resources, and you notice a significant amount of traffic from an IP address in a foreign country in which your company does not have customers. Further investigation of the traffic indicates the source of the traffic is scanning for open ports on your EC2-VPC instances. Which one of the following resources can deny the traffic from reaching the instances?

A. Security group

B. Network ACL

C. NAT instance

D. An Amazon VPC endpoint

17. Which of the following is the security protocol supported by Amazon VPC?

A. SSH

B. Advanced Encryption Standard (AES)

C. Point-to-Point Tunneling Protocol (PPTP)

D. IPsec

18. Which of the following Amazon VPC resources would you use in order for EC2-VPC instances to send traffic directly to Amazon S3?

A. Amazon S3 gateway

B. IGW

C. CGW

D. VPC endpoint

19. What properties of an Amazon VPC must be specified at the time of creation? (Choose 2 answers) A. The CIDR block representing the IP address range

B. One or more subnets for the Amazon VPC

C. The region for the Amazon VPC

D. Amazon VPC Peering relationships

20. Which Amazon VPC feature allows you to create a dual-homed instance?

A. EIP address

B. ENI

C. Security groups

D. CGW

Chapter 4: Amazon Virtual Private Cloud (Amazon VPC)

1. C. The minimum size subnet that you can have in an Amazon VPC is /28.
2. C. You need two public subnets (one for each Availability Zone) and two private subnets (one for each Availability Zone). Therefore, you need four subnets.
3. A. Network ACLs are associated to a VPC subnet to control traffic flow.
4. A. The maximum size subnet that you can have in a VPC is /16.
5. D. By creating a route out to the Internet using an IGW, you have made this subnet public.
6. A. When you create an Amazon VPC, a route table is created by default. You must manually create subnets and an IGW.
7. C. When you provision an Amazon VPC, all subnets can communicate with each other by default.
8. A. You may only have one IGW for each Amazon VPC.
9. B. Security groups are stateful, whereas network ACLs are stateless.
10. C. You should disable source/ destination checks on the NAT.
11. B, E. In the EC2-Classic network, the EIP will be disassociated with the instance; in the EC2-VPC network, the EIP remains associated with the instance. Regardless of the underlying network, a stop/ start of an Amazon EBS-backed Amazon EC2 instance always changes the host computer.
12. D. Six VPC Peering connections are needed for each of the four VPCs to send traffic to the other.
13. B. A DHCP option set allows customers to define DNS servers for DNS name resolution, establish domain names for instances within an Amazon VPC, define NTP servers, and define the NetBIOS name servers.
14. D. A CGW is the customer side of a VPN connection, and an IGW connects a network to the Internet.
15. A VPG is the Amazon side of a VPN connection. A. The default limit for the number of Amazon VPCs that a customer may have in a region is 5.
16. B. Network ACL rules can deny traffic.
17. D. IPsec is the security protocol supported by Amazon VPC.
18. D. An Amazon VPC endpoint enables you to create a private connection between your Amazon VPC and another AWS service without requiring access over the Internet or through a NAT device, VPN connection, or AWS Direct Connect.
19. A, C. The CIDR block is specified upon creation and cannot be changed. An Amazon VPC is associated with exactly one region which must be specified upon creation. You can add a subnet to an Amazon VPC any time after it has been created, provided its address range falls within the Amazon VPC CIDR block and does not overlap with the address range of any existing CIDR block. You can set up peering relationships between Amazon VPCs after they have been created.
20. B. Attaching an ENI associated with a different subnet to an instance can make the instance dual-homed.

4 장 : Amazon VPC (Amazon Virtual Private Cloud)

1. Amazon VPC에서 가질 수있는 최소 크기 서브넷은 / 28입니다.

2. 두 개의 공용 서브넷 (각 가용성 영역에 하나씩)과 두 개의 개인 서브넷 (각 가용성 영역에 하나씩)이 필요합니다. 따라서 네 개의 서브넷이 필요합니다.

3. A. 네트워크 ACL은 트래픽 흐름을 제어하기 위해 VPC 서브넷과 연결됩니다.

4. A. VPC에서 가질 수있는 최대 크기 서브넷은 / 16입니다.

5. IGW를 사용하여 인터넷에 경로를 생성함으로써이 서브넷을 공개하게 만들었습니다.

6. A. Amazon VPC를 만들면 기본적으로 경로 테이블이 만들어집니다. 서브넷과 IGW를 수동으로 만들어야합니다.

7. Amazon VPC를 프로비저닝 할 때 모든 서브넷은 기본적으로 서로 통신 할 수 있습니다.

8. A. Amazon VPC 당 하나의 IGW 만 가질 수 있습니다.

B. 보안 그룹은 상태 저장이지만 네트워크 ACL은 상태 저장이 아닙니다.

C. NAT에서 출발지 / 목적지 확인을 비활성화해야합니다.

11. B, E. EC2-Classic 네트워크에서 EIP는 인스턴스와의 연결을 끊습니다. EC2-VPC 네트워크에서 EIP는 인스턴스와 연관되어 있습니다. 기반 네트워크에 관계없이 Amazon EBS 지원 Amazon EC2 인스턴스의 중지 / 시작은 항상 호스트 컴퓨터를 변경합니다.

12. 6 개의 VPC 피어링 연결은 4 개의 VPC가 각각 다른 트래픽으로 트래픽을 전송하는 데 필요합니다.

B. DHCP 옵션 세트를 사용하면 DNS 이름 확인을위한 DNS 서버를 정의하고 Amazon VPC 내의 인스턴스에 대한 도메인 이름을 설정하고 NTP 서버를 정의하고 NetBIOS 이름 서버를 정의 할 수 있습니다.

14. D. CGW는 VPN 연결의 고객 측이고 IGW는 네트워크를 인터넷에 연결합니다.

15. VPG는 VPN 연결의 Amazon 측입니다. A. 한 지역에서 고객이 가질 수있는 Amazon VPC의 수에 대한 기본 한도는 5입니다.

16. 네트워크 ACL 규칙은 트래픽을 거부 할 수 있습니다.

17. D. IPsec은 Amazon VPC에서 지원하는 보안 프로토콜입니다.

18. D. Amazon VPC 엔드 포인트를 사용하면 인터넷이나 NAT 장치, VPN 연결 또는 AWS Direct Connect를 통한 액세스없이 Amazon VPC와 다른 AWS 서비스 사이에 개인 연결을 생성 할 수 있습니다.

19. A, C. CIDR 블록은 생성시 지정되며 변경할 수 없습니다. Amazon VPC는 ​​생성시 지정해야하는 정확히 하나의 영역과 연결됩니다. 서브넷은 주소 범위가 Amazon VPC CIDR 블록에 속하며 기존 CIDR 블록의 주소 범위와 겹치지 않는다면 언제든지 생성 된 후 언제든지 Amazon VPC에 추가 할 수 있습니다. 제작 된 Amazon VPC 간의 피어링 관계를 설정할 수 있습니다.

B. 다른 서브넷과 연결된 ENI를 인스턴스에 연결하면 해당 인스턴스가 이중 홈이 될 수 있습니다.