1) Your on-premises network has an IP address range of 11.11.0.0/16. Only IPs within this network range can be used for inter-server communication. The IP address range 11.11.253.0/24 has been allocated for the cloud.

You need to design a VPC in AWS. The servers within the VPC should be able to communicate with hosts both on the Internet and on-premises through a VPN connection.

What combination of configuration steps meets your needs? (Choose 2)

A) Set up the VPC with an IP address range of 11.11.253.0/24.
B) Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set up a NAT gateway to do translation between 10.10.10.0/24 and 11.11.253.0/24 for all outbound traffic.
C) Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for all traffic, and configure the on-premises router to forward traffic to the Internet.
D) Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for traffic destined to 11.11.0.0/24, and add a VPC subnet route to point the default gateway to an Internet gateway for Internet traffic.
E) Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set the VGW to do a source IP translation of all outbound packets to 11.11.0.0/16.

2) Your application server instances reside in the private subnet of your VPC. These instances need to access a Git repository on the Internet. You create a NAT gateway in the public subnet of your VPC. The NAT gateway can reach the Git repository, but instances in the private subnet cannot. You confirm that a default route in the private subnet route table points to the NAT gateway. The security group for your application server instances permits all traffic to the NAT gateway.

What configuration change should you make to ensure that these instances can reach the patch server?

A) Assign public IP addresses to the instances and route 0.0.0.0/0 to the Internet gateway.
B) Configure an outbound rule on the application server instance security group for the Git repository.
C) Configure inbound network access control lists (network ACLs) to allow traffic from the Git repository to the public subnet.
D) Configure an inbound rule on the application server instance security group for the Git repository.

3) Your company has installed an AWS Direct Connect connection in an ap-southeast-1 Direct Connect location. A public virtual interface is configured through a router to a dedicated firewall. You advertise your company's public /24 CIDR block to AWS with AS 65500. The company maintains a separate, corporate Internet firewall to map all outbound traffic to a single IP. This firewall maintains a BGP relationship with an upstream Internet provider that has delegated the public IP block your company uses. When the BGP session for the public virtual interface is up, corporate network users cannot access Amazon S3 resources in the ap-southeast-1 region.

Which step should you take to provide concurrent AWS and Internet access?

A) Configure AS-PATH prepending for the public virtual interface.
B) Advertise a host route for the corporate firewall on the public virtual interface.
C) Advertise a host route for the corporate firewall to the upstream Internet provider.
D) NAT the traffic destined for AWS from the dedicated firewall using the public virtual interface.

4) Your Amazon Kinesis application receives data streams from thousands of devices. The data is then stored in an on-premises Hadoop cluster. You are concerned about historical data that shows periods of sustained traffic between 1 Gbps and 2 Gbps during peaks. You must ensure that you have secure, fault-tolerant connectivity between Amazon Kinesis and your data center.

What should you implement to address these needs?

A) Deploy a single 1-Gbps Direct Connect connection with a VPN backup.
B) Deploy three 1-Gbps Direct Connect connections.
C) Deploy two 1-Gbps Direct Connect connections.
D) Set up an IPsec VPN connection over Direct Connect with two tunnels.

5) You have a web application (app.mycompany.com) running on an EC2 instance with a single elastic network interface in a subnet in a VPC. Because of a network redesign, you need to move the web application to a different subnet in the same Availability Zone.

Which of the following migration strategies meets the requirements?

A) Create an elastic network interface in the new subnet. Attach this interface to the instance, and detach the old interface.
B) Launch a new instance in the subnet via an AMI created from the instance, and redirect new connections to this new instance using DNS. Decommission the old instance.
C) Make an API call to change the subnet association of the elastic network interface.
D) Change the IP addresses manually to another subnet within the server operating system.

6) You are architecting your e-business application for PCI compliance. To meet the compliance requirements, you need to monitor web application logs to identify any malicious activity. You also need to monitor for remote attempts to change the network interface of web instances.

Which two AWS services will be helpful to achieve this goal?

A) Amazon CloudWatch Logs and VPC Flow Logs
B) AWS CloudTrail and VPC Flow Logs
C) AWS CloudTrail and CloudWatch Logs
D) AWS CloudTrail and AWS Config

7) You have an application that is processing confidential data. The data is currently stored in your data center. You are moving workloads to AWS, and you need to ensure confidentiality and integrity of the data in transit to your VPC. Your company has an existing AWS Direct Connect connection.

What combination of steps should you perform to set up the most cost-effective connection between your on-premises data center and AWS? (Choose 3)

A) Set up a VPC with a virtual private gateway.
B) Set up a VPC with an Internet gateway.
C) Configure a public virtual interface on your Direct Connect connection.
D) Configure a private virtual interface to the virtual private gateway.
E) Set up an IPsec tunnel between your customer gateway and a software VPN on Amazon EC2 in the VPC.
F) Set up an IPsec tunnel between your customer gateway appliance and the virtual private gateway.

8) You are deploying a web application in a VPC that requires SSL mutual authentication with a client-side, smartcard-stored certificate. The ELB Classic Load Balancer listener must support mutual authentication between the client and the application.

Which load balancer protocol should you select for this application?

A) HTTP
B) HTTPS
C) SSL

D) TCP

9) You are architecting an HPC solution in AWS. The system consists of a cluster of EC2 instances that require low-latency communications between them.

Which method should you use to set up a cluster to meet these requirements?

A) Create a VPC with one subnet in a single Availability Zone. Keep the size of the subnet equal to the number of instances required in the cluster. Launch instances for the cluster in this small subnet to guarantee low-latency network performance.
B) Create a placement group. Choose an EC2 instance type compatible with placement groups for the cluster. Launch instances for the cluster in the placement group.
C) Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach all instances to an Amazon EBS PIOPS volume. Implement a shared memory system across all instances in the cluster, using this shared EBS volume to minimize latency of communication.
D) Choose an EC2 instance type that offers enhanced networking. Attach a 10-Gbps non-blocking elastic network interface to the instances. Configure the elastic network interface to optimize network performance to reduce latency.

10) Your customer's internal security teams receive requests to allow Amazon S3 access from inside the corporate network. All external traffic must be explicitly whitelisted through your corporate firewalls.

How can your security team grant this access?

A) Obtain the list of IP prefixes from AWS Forum announcements, and use those prefixes in firewall rules.
B) Obtain the list of IP prefixes from ip-ranges.json, and use those prefixes in firewall rules.
C) Obtain the list of IP prefixes by performing a DNS lookup on Amazon S3 endpoints, and use those prefixes in firewall rules.
D) Connect your data center to a VPC via Direct Connect. Create routes that forward traffic from your data center to an S3 private endpoint.

Answers

1) A, C - The VPC needs to use a CIDR block in the assigned range (and be non-overlapping with the data center). All traffic not destined for the VPC is routed to the VGW (that route is assumed) and must then be forwarded to the Internet when it arrives on-premises. B and E are wrong because they are not in the assigned range (you can use non-RFC 1918 addresses in a VPC). D is wrong because it directs traffic to the Internet through the Internet gateway.

2) B - The traffic leaves the instance destined for the Git repository; at this point, the security group must allow it through. The route then directs that traffic (based on the IP) to the NAT gateway. A is wrong because it removes the private aspect of the subnet and would have no effect on the blocked traffic anyway. C is wrong because the problem is that outgoing traffic is not getting to the NAT gateway. D is wrong because to allow outgoing traffic to the Git repository requires an outgoing security group rule.

3) D - When outgoing traffic is routed via the corporate firewall, its return path is via the Direct Connect public virtual interface and therefore through the dedicated firewall. This dedicated firewall does not track the original NAT session and subsequently drops the traffic. Answer A is incorrect because AWS will always prefer Direct Connect over Internet routing. Answer B is incorrect because return traffic is still processed by the dedicated firewall. Answer C is incorrect because it does not change the traffic flow.

4) B - Three connections are required to provide fault tolerance. All of the other options would be unable to handle the peak loads over 1 Gbps without exceeding the available bandwidth.

5) B - Instances cannot change subnets, so a new instance must be created (Response B). A is wrong because you cannot remove the original elastic network interface. C is not possible. D is wrong because the OS has no ability to affect the AWS assigned IP addresses.

6) C - Web application logs are internal to the operating system, so the only way to monitor them with an AWS service is to export them using CloudWatch Logs. AWS CloudTrail monitors the API activity and can be used to watch for particular API calls. The correct answer is the only one that references both these services.

7) A, C, F - Setting up a VPN over your Direct Connect connection will secure the data in transit. The steps to do so are: adding a VGW to the VPC; setting up a public virtual interface; and creating the IPsec tunnel between your data center and the VGW via the public virtual interface. B would send traffic over the public Internet. D is not possible because a public virtual interface is needed to announce the VGW endpoint IPs. E would not take advantage of the already existing Direct Connect connection.

8) D - An ELB Classic Load Balancer cannot validate a client side certificate, so it must be passed through as standard TCP on port 443 to let the EC2 instance handle the validation.

9) B - Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. A is incorrect because the size of a subnet has no impact on network performance. C is incorrect because an EBS volume cannot be shared between EC2 instances. D is only half the solution because the enhanced networking affects the network behavior of an EC2 instance but not the network infrastructure between instances.

10) B - ip-ranges.json contains the latest list of IP addresses used by AWS. AWS no longer posts IP prefixes in Forum announcements. DNS lookups would not provide an exhaustive list of possible IP prefixes. D would require transitive routing, which is not possible.