1) A company's 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.

A network engineer needs to design a VPC on AWS. The servers within the VPC should be able to communicate with hosts both on the internet and on-premises through a VPN connection.

Which combination of configuration steps meet these requirements? (Select TWO.)

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 (for example, 10.10.10.0/24). 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 virtual private gateway and an on-premises router. Set the virtual private gateway as the default gateway for all traffic. Configure the on-premises router to forward traffic to the internet.
D) Set up a VPN connection between a virtual private gateway and an on-premises router. Set the virtual private gateway as the default gateway for traffic destined to 11.11.0.0/24. 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 (for example, 10.10.10.0/24). Set the virtual private gateway to do a source IP translation of all outbound packets to 11.11.0.0/16.

2) A network engineer needs to design a solution for an application running on an Amazon EC2 instance to connect to a publicly accessible Amazon RDS Multi-AZ DB instance in a different VPC and Region. Security requirements mandate that the traffic not traverse the internet.

Which configuration will ensure that the instances communicate privately without routing traffic over the internet?

A) Create a peering connection between the VPCs and update the routing tables to route traffic between the VPCs. Enable DNS resolution support for the VPC peering connection. Configure the application to connect to the DNS endpoint of the DB instance.
B) Create a gateway endpoint to the DB instance. Update the routing tables in the application VPC to route traffic to the gateway endpoint.
C) Configure a transit VPC to route traffic between the VPCs privately. Configure the application to connect to the DNS endpoint of the DB instance.
D) Create a NAT gateway in the same subnet as the EC2 instances. Update the routing tables in the application VPC to route traffic through the NAT gateway to the DNS endpoint of the DB instance.

3) A company has implemented a critical environment on AWS. For compliance purposes, a network engineer needs to verify that the Amazon EC2 instances are using a specific approved security group and belong to a specific VPC. The configuration history of the instances should be recorded and, in the event of any compliance issues, the instances should be automatically stopped.

What should be done to meet these requirements?

A) Enable AWS CloudTrail and create a custom Amazon CloudWatch alarm to perform the required checks. When the CloudWatch alarm is in a failed state, trigger the stop this instance action to stop the noncompliant EC2 instance.
B) Configure a scheduled event with AWS CloudWatch Events to invoke an AWS Lambda function to perform the required checks. In the event of a noncompliant resource, invoke another Lambda function to stop the EC2 instance.
C) Configure an event with AWS CloudWatch Events for an EC2 instance state-change notification that triggers an AWS Lambda function to perform the required checks. In the event of a noncompliant resource, invoke another Lambda function to stop the EC2 instance.
D) Enable AWS Config and create custom AWS Config rules to perform the required checks. In the event of a noncompliant resource, use a remediation action to execute an AWS Systems Manager document to stop the EC2 instance.

4) A company is extending its on-premises data center to AWS. Peak traffic is expected to range between 1 Gbps and 2 Gbps. A network engineer must ensure that there is sufficient bandwidth between AWS and the data center to handle peak traffic. The solution should be highly available and cost effective.

What should be implemented to address these needs?

A) Deploy a 10 Gbps AWS Direct Connect connection with an IPsec VPN backup.
B) Deploy two 1 Gbps AWS Direct Connect connections in a link aggregation group.
C) Deploy two 1 Gbps AWS Direct Connect connections in a link aggregation group to two different Direct Connect locations.
D) Deploy a 10 Gbps AWS Direct Connect connection to two different Direct Connect locations.

5) A network engineer needs to limit access to the company's Amazon S3 bucket to specific source networks.

What should the network engineer do to accomplish this?

A) Create an ACL on the S3 bucket, limiting access to the CIDR blocks of the specified networks.
B) Create a bucket policy on the S3 bucket, limiting access to the CIDR blocks of the specified networks using a condition statement.
C) Create a security group allowing inbound access to the CIDR blocks of the specified networks and apply the security group to the S3 bucket.
D) Create a security group allowing inbound access to the CIDR blocks of the specified networks, create a S3 VPC endpoint, and apply the security group to the VPC endpoint.

6) A company's compliance requirements specify that web application logs must be collected and analyzed to identify any malicious activity. A network engineer also needs to monitor for remote attempts to change the network interface of web instances.

Which services and configurations will meet these requirements?

A) Install the Amazon CloudWatch Logs agent on the web instances to collect application logs. Use VPC Flow Logs to send data to CloudWatch Logs. Use CloudWatch Logs metric filters to define the patterns to look for in the log data.
B) Configure AWS CloudTrail to log all management and data events to a custom Amazon S3 bucket and Amazon CloudWatch Logs. Use VPC Flow Logs to send data to CloudWatch Logs. Use CloudWatch Logs metric filters to define the patterns to look for in the log data.
C) Configure AWS CloudTrail to log all management events to a custom Amazon S3 bucket and Amazon CloudWatch Logs. Install the Amazon CloudWatch Logs agent on the web instances to collect application logs. Use CloudWatch Logs Insights to define the patterns to look for in the log data.
D) Enable AWS Config to record all configuration changes to the web instances. Configure AWS CloudTrail to log all management and data events to a custom Amazon S3 bucket. Use Amazon Athena to define the patterns to look for in the log data stored in Amazon S3.

7) A company has an application that processes confidential data. The data is currently stored in an on-premises data center. A network engineer is moving workloads to AWS, and needs to ensure confidentiality and integrity of the data in transit to AWS. The company has an existing AWS Direct Connect connection.

Which combination of steps should the network engineer perform to set up the most cost-effective connection between the on-premises data center and AWS? (Select TWO.)

A) Attach an internet gateway to the VPC.
B) Configure a public virtual interface on the AWS Direct Connect connection.
C) Configure a private virtual interface to the virtual private gateway.
D) Set up an IPsec tunnel between the customer gateway and a software VPN on Amazon EC2.
E) Set up a Site-to-Site VPN between the customer gateway and the virtual private gateway.

8) A company is creating new features for its ecommerce website. These features will be deployed as microservices using different domain names for each service. The company requires the use of HTTPS for all its public-facing websites. The application requires the client's source IP.

Which combination of actions should be taken to accomplish this? (Select TWO.)

A) Use a Network Load Balancer to distribute traffic to each service.
B) Use an Application Load Balancer to distribute traffic to each service.
C) Configure the application to retrieve client IPs using the X-Forwarded-For header.
D) Configure the application to retrieve client IPs using the X-Forwarded-Host header.
E) Configure the application to retrieve client IPs using the PROXY protocol header.

9) A network engineer is architecting a high performance computing solution on AWS. The system consists of a cluster of Amazon EC2 instances that require low-latency communications between them.

Which method will meet these requirements?

A) Launch instances into a single subnet with a size equal to the number of instances required for the cluster.
B) Create a cluster placement group. Launch Elastic Fabric Adapter (EFA)-enabled instances into the placement group.
C) Launch Amazon EC2 instances with the largest available number of cores and RAM. Attach Amazon EBS Provisioned IOPS (PIOPS) volumes. Implement a shared memory system across all instances in the cluster.
D) Choose an Amazon EC2 instance type that offers enhanced networking. Attach a 10 Gbps non-blocking elastic network interface to the instances.

10) A company's internal security team receives a request to allow Amazon S3 access from inside the corporate network. All external traffic must be explicitly allowed through the corporate firewalls.

How can the security team grant this access?

A) Schedule a script to download the Amazon S3 IP prefixes from AWS developer forum announcements. Update the firewall rules accordingly.
B) Schedule a script to download and parse the Amazon S3 IP prefixes from the ip-ranges.json file. Update the firewall rules accordingly.
C) Schedule a script to perform a DNS lookup on Amazon S3 endpoints. Update the firewall rules accordingly.
D) Connect the data center to a VPC using AWS Direct Connect. Create routes that forward traffic from the data center to an Amazon S3 VPC 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 virtual private gateway (that route is assumed) and must then be forwarded to the internet when it arrives on-premises. B and E are incorrect because they are not in the assigned range (non-RFC 1918 addresses can be used in a VPC). D is incorrect because it directs traffic to the internet through the internet gateway.

2) A - Configuring DNS resolution on the VPC peering connection will allow queries from the application VPC to resolve to the private IP of the DB instance and prevent routing over the internet. B is incorrect because Amazon RDS is not supported by gateway endpoints. C and D are incorrect because the database endpoint will resolve to a public IP and the traffic will go over the internet.

3) D - AWS Config provides a detailed view of the configuration of AWS resources in a user's AWS account. Using AWS Config rules with AWS Systems Manager Automation documents can automatically remediate noncompliant resources.

4) C - Two AWS Direct Connect connections with link aggregation groups in two different Direct Connect locations are required to provide sufficient bandwidth with high availability. If one Direct Connect location experiences a failure, the two Direct Connect connections in the second Direct Connect location will provide backup. All of the other options would be unable to handle the peak traffic if a connection was lost.

5) B - An Amazon S3 bucket policy that uses a condition statement will support restricting access if the request originates from a specific range of IP addresses. A is incorrect because an S3 ACL does not support IP restrictions. C is incorrect because security groups cannot be applied to S3 buckets. D is incorrect because security groups cannot be applied to an S3 VPC endpoint.

6) C - Web application logs are internal to the operating system, and Amazon CloudWatch Logs Insights can be used to collect and analyze the logs using the CloudWatch agent. AWS CloudTrail monitors all AWS API activity and can be used to monitor particular API calls to identify remote attempts to change the network interface of web instances.

7) B, E - Setting up a VPN over an AWS Direct Connect connection will secure the data in transit. The steps to do so are: set up a public virtual interface and create the Site-to-Site VPN between the data center and the virtual private gateway using the public virtual interface. A is incorrect because it would send traffic over the public internet. C is not possible because a public virtual interface is needed to announce the VPN tunnel IPs. D is incorrect because it would not take advantage of the already existing Direct Connect connection.

8) B, C - An Application Load Balancer supports host-based routing, which is required to route traffic to different microservices based on the domain name. X-Forwarded-For is the correct request header to identify the client's source IP address.

9) B - Cluster placement groups and Elastic Fabric Adapters (EFAs) are recommended for high performance computing 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 Amazon EBS volume cannot be shared between Amazon 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 - The ip-ranges.json file contains the latest list of IP addresses used by AWS. AWS no longer posts IP prefixes in developer forum announcements. DNS lookups would not provide an exhaustive list of possible IP prefixes. D would require transitive routing, which is not possible.