1) A gaming company is planning to launch a globally available game that is hosted in one AWS Region. The game backend is hosted on Amazon EC2 instances that are part of an Auto Scaling group. The game uses the gRPC protocol for bidirectional streaming between game clients and the backend. The company needs to filter incoming traffic based on the source IP address to protect the game.

Which solution will meet these requirements?

A) Configure an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
B) Configure an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.
C) Configure an Amazon CloudFront distribution with an Application Load Balancer (ALB) endpoint. Attach the ALB to the Auto Scaling group. Configure an AWS WAF web ACL for the ALB to filter traffic based on the source IP address.
D) Configure an Amazon CloudFront distribution with a Network Load Balancer (NLB) endpoint. Attach the NLB to the Auto Scaling group. Configure security groups for the EC2 instances to filter traffic based on the source IP address.

2) A company has multiple VPCs in the us-east-1 Region. The company has deployed a website in one of the VPCs. The company wants to implement split-view DNS so that the website is accessible internally from the VPCs and externally over the internet with the same domain name, example.com.

Which solution will meet these requirements?

A) Change the DHCP options for each VPC to use the IP address of an on-premises DNS server. Create a private hosted zone and a public hosted zone for example.com. Map the private hosted zone to the website's internal IP address. Map the public hosted zone to the website's external IP address.
B) Create Amazon Route 53 private hosted zones and public hosted zones that have the same name, example.com. Associate the VPCs with the private hosted zone. Create records in each hosted zone that determine how traffic is routed.
C) Create an Amazon Route 53 Resolver inbound endpoint for resolving example.com internally. Create a Route 53 public hosted zone for routing external DNS queries.
D) Create an Amazon Route 53 Resolver outbound endpoint for resolving example.com externally. Create a Route 53 private hosted zone for routing internal DNS queries.

3) A company has developed a new web application that processes confidential data that is hosted on Amazon EC2 instances. The application needs to scale and must use certificates to authenticate clients. The application is configured to request a client's certificate and will validate the certificate as part of the initial handshake.

Which Elastic Load Balancing (ELB) solution will meet these requirements?

A) Configure an Application Load Balancer (ALB) that includes an HTTPS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure HTTPS as the protocol for the target group.
B) Configure a Network Load Balancer (NLB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure the NLB to terminate TLS. Configure TLS as the protocol for the target group.
C) Configure a Network Load Balancer (NLB) that includes a TCP listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the NLB. Configure TCP as the protocol for the target group.
D) Configure an Application Load Balancer (ALB) that includes a TLS listener on port 443. Create an Auto Scaling group for the EC2 instances. Configure the Auto Scaling group as the target group of the ALB. Configure TLS as the protocol for the target group.

4) A company collects a high volume of shipping data and stores the data in an on-premises data center. A network engineer wants to use Amazon S3 to store the data during the first phase of a migration to AWS. During this phase, an application that resides in the data center will need to access the data privately in an S3 bucket that the company created.

The company has set up an AWS Direct Connect connection with a private VIF to connect the on-premises data center to a VPC. The network engineer plans to use this Direct Connect connection for the hybrid cloud setup. The solution must be highly available.

What should the network engineer do next to implement this architecture?

A) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure the S3 gateway endpoint DNS name in the on-premises application.
B) Configure an S3 interface endpoint in the VPC. Configure the S3 interface endpoint DNS name in the on-premises application.
C) Configure an S3 gateway endpoint in the VPC. Update VPC route tables to route traffic to the S3 gateway endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 gateway endpoint. Configure the HTTP proxy DNS name in the on-premises application.
D) Configure an S3 interface endpoint in the VPC. Update VPC route tables to route traffic to the S3 interface endpoint. Configure an HTTP proxy on an Amazon EC2 instance in the VPC to route traffic to the S3 interface endpoint. Configure the HTTP proxy DNS name in the on-premises application.

5) A company is designing infrastructure on AWS with three VPCs connected to a transit gateway. The three VPCs are an application VPC, a backend VPC, and an inspection VPC. The application VPC and the backend VPC have compute instances deployed in Availability Zone A and Availability Zone B. Stateful firewalls are deployed in the same Availability Zones in the inspection VPC, which is a shared services VPC.

All traffic is routed through the inspection VPC through the stateful layer 7 virtual firewall appliances to comply with a security policy that mandates traffic inspection. There are no overlapping IP addresses across the three VPCs. A network engineer must ensure that traffic between the application VPC and the backend VPC can route through the inspection VPC's stateful firewalls.

Which solution will meet these requirements?

A) Create IPsec VPN connections between the transit gateway and the virtual firewall appliances.
B) Configure Virtual Router Redundancy Protocol (VRRP) on the virtual firewall appliances.
C) Set up BGP between the transit gateway and the virtual firewall appliances.
D) Enable transit gateway appliance mode for the VPC attachment to the inspection VPC.

6) A company hosts a public hosted zone in Amazon Route 53. The company wants to configure DNS Security Extensions (DNSSEC) signing for the public hosted zone. All the company's business-critical applications are running in the us-west-2 Region.

The company has created a symmetric, customer managed, single-Region key in us-west-2 by using AWS Key Management Service (AWS KMS). A network engineer finds that the existing AWS KMS key cannot be used to create a key-signing key (KSK).

How can the network engineer resolve this issue?

A) Recreate a symmetric, customer managed, multi-Region key in the us-east-1 Region. Use this key to create a KSK.
B) Recreate a symmetric, customer managed, single-Region key in us-west-2. Use this key to create a KSK.
C) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in the us-east-1 Region. Use this key to create a KSK.
D) Recreate an asymmetric, customer managed key with an ECC_NIST_P256 key spec in us-west-2. Use this key to create a KSK.

7) A company is migrating many applications from two on-premises data centers to AWS. The company's network team is setting up connectivity to the AWS environment. The migration will involve spreading the applications across two AWS Regions: us-east-1 and us-west-2. The company has set up AWS Direct Connect connections at two different locations. Direct Connect connection 1 is to the first data center and is at a location in us-east-1. Direct Connect connection 2 is to the second data center and is at a location in us-west-2.

The company has connected both Direct Connect connections to a single Direct Connect gateway by using transit VIFs. The Direct Connect gateway is associated with transit gateways that are deployed in each Region. All traffic to and from AWS must travel through the first data center. In the event of failure, the second data center must take over the traffic.

How should the network team configure BGP to meet these requirements?

A) Configure the local preference BGP community tag 7224:7300 for the transit VIF connected to Direct Connect connection 2.
B) Configure the local preference BGP community tag 7224:9300 for the transit VIF connected to Direct Connect connection 2.
C) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 2.
D) Use the AS_PATH attribute to prepend the additional hop for the transit VIF connected to Direct Connect connection 1.

8) An ecommerce company has a business-critical application that runs on Amazon EC2 instances in a VPC. The company's development team has been testing a new version of the application on test EC2 instances. The development team wants to test the new application version against production traffic to address any problems that might occur before the company releases the new version across all servers.

Which solution will meet this requirement with no impact on the end user's experience?

A) Configure Amazon Route 53 weighted routing policies by configuring records that have the same name and type as each of the instances. Assign relative weights to the production instances and the test instances.
B) Create an Application Load Balancer with weighted target groups. Add more than one target group to the forward action of a listener rule. Specify a weight for each target group.
C) Implement Traffic Mirroring to replay the production requests to the test instances. Configure the source as the production instances. Configure the target as the test instances.
D) Configure an NGINX proxy in front of the production servers. Use the NGINX mirroring capability.

9) A company hosts its ecommerce application on Amazon EC2 instances behind an Application Load Balancer. The EC2 instances are in a private subnet with the default DHCP options set. Internet connectivity is through a NAT gateway that is configured in the public subnet.

A third-party audit of the security infrastructure identifies a DNS exfiltration vulnerability. The company must implement a highly available solution that protects against this vulnerability.

Which solution will meet these requirements MOST cost-effectively?

A) Configure a BIND server with DNS filtering. Modify the DNS servers in the DHCP options set.
B) Use Amazon Route 53 Resolver DNS Firewall. Configure a domain list with a rule group.
C) Use AWS Network Firewall with domain name filtering.
D) Configure an Amazon Route 53 Resolver outbound endpoint with rules to filter and block suspicious traffic.

10) A company is using Amazon Route 53 Resolver for its hybrid DNS infrastructure. The company is using Route 53 Resolver forwarding rules for authoritative domains that are hosted on on-premises DNS servers. The company achieves hybrid network connectivity by using an AWS Site-to-Site VPN connection.

A new governance policy requires logging for DNS traffic that originates in the AWS Cloud. The policy also requires the company to query DNS traffic to identify the source IP address of the resources that the query originated from, along with the DNS name that was requested.

Which solution will meet these requirements?

A) Create VPC flow logs for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.
B) Configure Route 53 Resolver query logging for all VPCs. Send the logs to Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the IP address and DNS name.
C) Configure DNS logging for the Site-to-Site VPN connection. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.
D) Modify the existing Route 53 Resolver rules to configure logging. Send the logs to an Amazon S3 bucket. Use Amazon Athena to query the IP address and DNS name.

Answers

1) A **–** The accelerator in AWS Global Accelerator will project low-latency endpoints to the global users of the game. The accelerator also will route the traffic over the AWS network backbone to the AWS Region that is hosting the game. The Application Load Balancer (ALB) will support the use of the gRPC protocol and client IP address preservation. The ALB will distribute traffic to the Amazon EC2 instances in the Auto Scaling group to support the game's load and will provide an endpoint that will support the accelerator. The association of an AWS WAF web ACL with the ALB will provide the required IP filtering.

The other answer options do not meet the requirements. A Network Load Balancer does not support client IP address preservation, and Amazon CloudFront does not support the gRPC protocol.

2) B **–** The solution requires split-view DNS, which is directly supported by Amazon Route 53. You can configure split-view DNS by creating public hosted zones and private hosted zones in Route 53 with the same name. If the private hosted zones are associated with VPCs, Route 53 Resolver will use the private hosted zones to answer queries from those VPCs and will use the public hosted zones to answer public queries.

The other answer options will not work. An on-premises DNS server will not be able to replace Route 53 Resolver for operations within the VPC. A Resolver inbound endpoint will allow on-premises queries from on-premises networks to be resolved. A Resolver outbound endpoint is used to resolve queries from the VPC for on-premises addresses. Neither of those Resolver endpoints will provide the necessary public and internal resolution.

3) C **–** The application must scale to handle load and must use client certificates to authenticate directly with a web server. The solution requires the TLS sessions to be connected to the underlying web server or web servers. The need to scale requires the use of an Auto Scaling group with a load balancer. The load balancer must pass the TLS sessions to the Amazon EC2 instances. This architecture is supported by a Network Load Balancer (NLB) with a TCP listener on port 443. The NLB operates at the transport layer of the stack to pass the connection through to the web servers.

The other answer options will end the TLS connection from the client at the load balancer. These options will not allow the client certificate to be visible to the web servers. The NLB with a TCP listener on port 443 is the only option that will maintain the session all the way from the client to the web servers in the Auto Scaling group.

4) B **–** The question requires a solution that will provide a connection to Amazon S3 from workloads on AWS and from an on-premises data center. An S3 interface endpoint will provide the needed access from workloads on AWS and can support connections from the on-premises environment over AWS Direct Connect. The use of the S3 interface endpoint will require the on-premises client applications to use the endpoint DNS records.

Option A includes the use of a gateway endpoint. Routing to the gateway endpoint depends on the route tables of the VPC, and route tables do not support the use of DNS endpoints for the on-premises application. While option C could route the traffic, this option contains a single point of failure in the HTTP proxy server and does not offer the high availability that the question requires. Option D also contains an HTTP proxy, which is unneeded and creates a single point of failure. This option also includes the use of an interface endpoint name in a route table, which is incorrect.

5) D **–** The correct answer is to enable transit gateway appliance mode for the VPC attachment to the inspection VPC. The underlying issue in the question comes from cross-AZ traffic. When appliance mode is not enabled, a transit gateway attempts to keep traffic routed between VPC attachments in the originating Availability Zone until the traffic reaches its destination. This behavior causes return traffic to be routed to the virtual firewall in the firewall's local Availability Zone rather than to the Availability Zone that initiated the traffic. This discrepancy causes the firewall to drop the traffic.

Option A will create unnecessary connections and will not provide the symmetry that is needed for the traffic to flow through the firewalls. Option B includes the use of Virtual Router Redundancy Protocol (VRRP) for instance load sharing. AWS does not directly support this protocol, which depends on multicast. Multicast is not supported within a VPC. Option C is incorrect because virtual firewall appliances cannot use BGP peering with a transit gateway.

6) C – When Amazon Route 53 creates a key-signing key (KSK), Route 53 requires you to provide a customer managed key. The customer managed key must be located in the us-east-1 Region. The key must be an asymmetric customer managed key with an ECC_NIST_P256 key spec.

The other answer options are incorrect for a combination of two reasons. Option A includes a symmetric key, which violates the requirement for an asymmetric key. Option D correctly includes the asymmetric key, but the key is in the wrong Region. Option B has the wrong key and the wrong Region. Only keys that meet all the requirements can be used to create the KSK and support DNSSEC signing in Route 53.

7) A **–** The correct answer is to configure the local BGP community tag 7224:7300 for the transit VIF connected to the second AWS Direct Connect connection. By default, AWS uses the distance from the local AWS Region to the Direct Connect location to determine the VIF or transit VIF for routing. You can modify this behavior by assigning local preference communities to VIFs. This question asks for the VIF in Direct Connect connection 2 to have a higher preference. AWS supports the 7224:7300 local preference tag for high-preference use cases.

Option B includes the 7224:9300 community tag, which is used to control how far a customer-advertised prefix is propagated. This community tag will not help solve this routing priority problem. The remaining answer options propose the use of the AS_PATH attribute to control the traffic between Direct Connect connections in multiple Regions. This strategy would be appropriate for handling multiple VIFs in a single Region, but this strategy is not appropriate for handling multiple VIFs in this question's multi-Region environment.

8) C **–** Traffic Mirroring is the correct answer. Because this mirroring will occur at the transport layer, all the inbound requests can be captured and mirrored into a test environment without affecting the performance of the production environment. This solution will eliminate any possibility of a user encountering an error that is caused by a test of the new version. The existing production environment will serve all user requests.

The other answer options will either expose some of the users to the new version of the application or will add overhead and a potential failure point. The question requires the solution to have no impact on an end user's experience. By exposing the users to potential errors or performance problems, these options will produce a negative impact.

9) B **–** With Amazon Route 53 Resolver DNS Firewall, you can monitor and control the domains that applications in your VPCs can access. DNS Firewall supports the use of allow lists or deny lists to filter the set of domains that you can use. This solution can effectively prevent the use of DNS queries to exfiltrate data.

In option A, the configuration of a BIND server with DNS filtering could work. However, a single BIND server would be a single point of failure. Additionally, a fleet of BIND servers with load balancers would be more complex and expensive than the correct answer.

In option C, AWS Network Firewall provides filtering of application layer traffic and network layer traffic. However, Network Firewall does not have visibility into queries from Route 53 Resolver. Option D includes the configuration of a Route 53 Resolver outbound endpoint, which is used to forward queries for specific domains to an on-premises DNS server. However, this endpoint does not filter or block traffic.

10) B **–** The correct answer is to configure Amazon Route 53 Resolver query logging for all the VPCs. The query logs can be stored in Amazon CloudWatch Logs and can be analyzed with CloudWatch Logs Insights.

The other answer options will fail to capture the needed DNS queries. In option A, flow logs will fail to capture traffic from the Amazon EC2 instances to the Amazon provided DNS servers. In option C, AWS Site-to-Site VPN connections do not offer an option for DNS logging. In option D, Route 53 Resolver rules do not allow the configuration of logging.