# Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

**https://www.2passeasy.com/dumps/AWS-Certified-Advanced-Networking-Specialty/**

**NEW QUESTION 1**
A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instance hosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default network ACL with no modification applied. The EC2 instance has the default security group with no modification applied.
The SQS queue is not receiving messages.
Which of the following are possible causes of this problem? (Choose two.)

A. The EC2 instance is not attached to an IAM role that allows write operations to Amazon SQS.
B. The security group is blocking traffic to the IP address range used by Amazon SQS
C. There is no interface VPC endpoint configured for Amazon SQS
D. The network ACL is blocking return traffic from Amazon SQS
E. There is no route configured in the subnet route table for the IP address range used by Amazon SQS

**Answer:** CE

**NEW QUESTION 2**
A retail company is running its service on AWS. The company’s architecture includes Application Load Balancers (ALBs) in public subnets. The ALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can call externally hosted services over the internet by using a NAT gateway.
The company has noticed in its billing that NAT gateway usage has increased significantly. A network engineer needs to find out the source of this increased usage.
Which options can the network engineer use to investigate the traffic through the NAT gateway? (Choose two.)

A. Enable VPC flow logs on the NAT gateway's elastic network interfac
B. Publish the logs to a log group in Amazon CloudWatch Log
C. Use CloudWatch Logs Insights to query and analyze the logs.
D. Enable NAT gateway access log
E. Publish the logs to a log group in Amazon CloudWatch Log
F. Use CloudWatch Logs Insights to query and analyze the logs.
G. Configure Traffic Mirroring on the NAT gateway's elastic network interfac
H. Send the traffic to an additional EC2 instanc
I. Use tools such as tcpdump and Wireshark to query and analyze the mirrored traffic.
J. Enable VPC flow logs on the NAT gateway's elastic network interfac
K. Publish the logs to an Amazon S3 bucke
L. Create a custom table for the S3 bucket in Amazon Athena to describe the log structur
M. Use Athena to query and analyze the logs.
N. Enable NAT gateway access log
O. Publish the logs to an Amazon S3 bucke
P. Create a custom table for the S3 bucket in Amazon Athena to describe the log structur
Q. Use Athena to query and analyze the logs.

**Answer:** AD

**Explanation:**
To investigate the increased usage of a NAT gateway in a VPC architecture with ALBs and backend EC2 instances, a network engineer can use the following options:

- Enable VPC flow logs on the NAT gateway’s elastic network interface and publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query and analyze the logs.
(Option A)
- Enable VPC flow logs on the NAT gateway’s elastic network interface and publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athena to describe the log structure and use Athena to query and analyze the logs. (Option D)

These options allow for detailed analysis of traffic through the NAT gateway to identify the source of increased usage.

**NEW QUESTION 3**
A government contractor is designing a multi-account environment with multiple VPCs for a customer. A network security policy requires all traffic between any two VPCs to be transparently inspected by a
third-party appliance.
The customer wants a solution that features AWS Transit Gateway. The setup must be highly available across multiple Availability Zones, and the solution needs to support automated failover. Furthermore, asymmetric routing is not supported by the inspection appliances.
Which combination of steps is part of a solution that meets these requirements? (Choose two.)

A. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VP
B. Connect the inspection VPC to the transit gateway by using a VPCattachmen
C. Create a target group, and register the appliances with the target grou
D. Create a Network Load Balancer (NLB), and set it up to forward to the newly created target grou
E. Configure a default route in the inspection VPCs transit gateway subnet toward the NLB.
F. Deploy two clusters that consist of multiple appliances across multiple Availability Zones in a designated inspection VP
G. Connect the inspection VPC to the transit gateway by using a VPC attachmen
H. Create a target group, and register the appliances with the target grou
I. Create a Gateway Load Balancer, and set it up to forward to the newly created target grou
J. Configure a default route in the inspection VPC’s transit gateway subnet toward the Gateway Load Balancer endpoint.
K. Configure two route tables on the transit gatewa
L. Associate one route table with all the attachments of the application VPC
M. Associate the other route table with the inspection VPC’s attachmen
N. Propagate all VPC attachments into the inspection route tabl
O. Define a static default route in the application route tabl
P. Enable appliance mode on the attachment that connects the inspection VPC.
Q. Configure two route tables on the transit gatewa

R. Associate one route table with all the attachments of the application VPC
S. Associate the other route table with the inspection VPCs attachmen
T. Propagate all VPC attachments into the application route tabl
. Define a static default route in the inspection route tabl
. Enable appliance mode on the attachment that connects the inspection VPC.
. Configure one route table on the transit gatewa
. Associate the route table with all the VPC
. Propagate all VPC attachments into the route tabl
. Define a static default route in the route table.

**Answer:** BC

**NEW QUESTION 4**
An ecommerce company is hosting a web application on Amazon EC2 instances to handle continuously changing customer demand. The EC2 instances are part of an Auto Scaling group. The company wants to implement a solution to distribute traffic from customers to the EC2 instances. The company must encrypt all traffic at all stages between the customers and the application servers. No decryption at intermediate points is allowed.
Which solution will meet these requirements?

A. Create an Application Load Balancer (ALB). Add an HTTPS listener to the AL
B. Configure the Auto Scaling group to register instances with the ALB's target group.
C. Create an Amazon CloudFront distributio
D. Configure the distribution with a custom SSL/TLS certificat
E. Set the Auto Scaling group as the distribution's origin.
F. Create a Network Load Balancer (NLB). Add a TCP listener to the NL
G. Configure the Auto Scaling group to register instances with the NLB's target group.
H. Create a Gateway Load Balancer (GLB). Configure the Auto Scaling group to register instances with the GLB's target group.

**Answer:** C

**Explanation:**
To distribute traffic from customers to EC2 instances in an Auto Scaling group and encrypt all traffic at all stages between the customers and the application servers without decryption at intermediate points, the company should create a Network Load Balancer (NLB) with a TCP listener and configure the Auto Scaling group to register instances with the NLB’s target group (Option C). This solution allows for end-to-end encryption of traffic without decryption at intermediate points.

**NEW QUESTION 5**
An IoT company sells hardware sensor modules that periodically send out temperature, humidity, pressure, and location data through the MQTT messaging protocol. The hardware sensor modules send this data to the company's on-premises MQTT brokers that run on Linux servers behind a load balancer. The hardware sensor modules have been hardcoded with public IP addresses to reach the brokers.
The company is growing and is acquiring customers across the world. The existing solution can no longer scale and is introducing additional latency because of the company's global presence. As a result, the company decides to migrate its entire infrastructure from on premises to the AWS Cloud. The company needs to migrate without reconfiguring the hardware sensor modules that are already deployed across the world. The solution also must minimize latency.
The company migrates the MQTT brokers to run on Amazon EC2 instances. What should the company do next to meet these requirements?

A. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listener
B. Use Bring Your Own IP (BYOIP) from the on-premises network with the NLB.
C. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listener
D. Create an AWS Global Accelerator accelerator in front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator.
E. Place the EC2 instances behind an Application Load Balancer (ALB). Configure TCP listener
F. Create an AWS Global Accelerator accelerator in front of the AL
G. Use Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator
H. Place the EC2 instances behind an Amazon CloudFront distributio
I. Use Bring Your Own IP (BYOIP) from the on-premises network with CloudFront.

**Answer:** B

**NEW QUESTION 6**
A company has an AWS Site-to-Site VPN connection between its existing VPC and on-premises network. The default DHCP options set is associated with the VPC. The company has an application that is running on an Amazon Linux 2 Amazon EC2 instance in the VPC. The application must retrieve an Amazon RDS database secret that is stored in AWS Secrets Manager through a private VPC endpoint. An on-premises application provides internal RESTful API service that can be reached by URL (https://api.example.internal). Two on-premises Windows DNS servers provide internal DNS resolution.
The application on the EC2 instance needs to call the internal API service that is deployed in the on-premises environment. When the application on the EC2 instance attempts to call the internal API service by referring to the hostname that is assigned to the service, the call fails. When a network engineer tests the API service call from the same EC2 instance by using the API service's IP address, the call is successful.
What should the network engineer do to resolve this issue and prevent the same problem from affecting other resources in the VPC?

A. Create a new DHCP options set that specifies the on-premises Windows DNS server
B. Associate the new DHCP options set with the existing VP
C. Reboot the Amazon Linux 2 EC2 instance.
D. Create an Amazon Route 53 Resolver rul
E. Associate the rule with the VP
F. Configure the rule to forward DNS queries to the on-premises Windows DNS servers if the domain name matches example.internal.
G. Modify the local host file in the Amazon Linux 2 EC2 instance in the VPMap the service domain name (api.example.internal) to the IP address of the internal API service.
H. Modify the local /etc/resolv.conf file in the Amazon Linux 2 EC2 instance in the VP
I. Change the IP addresses of the name servers in the file to the IP addresses of the company's on-premises Windows DNS servers.

**Answer:** B

**Explanation:**

Creating an Amazon Route 53 Resolver rule and associating it with the VPC would enable forwarding of DNS queries for a specified domain name (example.internal) to a specified IP address (the on-premises Windows DNS servers)3. This would allow EC2 instances in the VPC to resolve the internal API service by using its hostname. Configuring the rule to forward DNS queries only if the domain name matches example.internal would also allow EC2 instances to use the Amazon Route 53 Resolver server for other DNS queries, such as those for AWS services through private VPC endpoints2.

**NEW QUESTION 7**
A company has developed an application on AWS that will track inventory levels of vending machines and initiate the restocking process automatically. The company plans to integrate this application with vending machines and deploy the vending machines in several markets around the world. The application resides in a VPC in the us-east-1 Region. The application consists of an Amazon Elastic Container Service (Amazon ECS) cluster behind an Application Load Balancer (ALB). The communication from the vending machines to the application happens over HTTPS.
The company is planning to use an AWS Global Accelerator accelerator and configure static IP addresses of the accelerator in the vending machines for application endpoint access. The application must be accessible only through the accelerator and not through a direct connection over the internet to the ALB endpoint.
Which solution will meet these requirements?

A. Configure the ALB in a private subnet of the VP
B. Attach an internet gateway without adding routes in the subnet route tables to point to the internet gatewa
C. Configure the accelerator with endpoint groups that include the ALB endpoin
D. Configure the ALB’s security group to only allow inbound traffic from the internet on the ALB listener port.
E. Configure the ALB in a private subnet of the VP
F. Configure the accelerator with endpoint groups that include the ALB endpoin
G. Configure the ALB's security group to only allow inbound traffic from the internet on the ALB listener port.
H. Configure the ALB in a public subnet of the VPAttach an internet gatewa
I. Add routes in the subnet route tables to point to the internet gatewa
J. Configure the accelerator with endpoint groups that include the ALB endpoin
K. Configure the ALB's security group to only allow inbound traffic from the accelerator's IP addresses on the ALB listener port.
L. Configure the ALB in a private subnet of the VP
M. Attach an internet gatewa
N. Add routes in the subnet route tables to point to the internet gatewa
O. Configure the accelerator with endpoint groups that include the ALB endpoin
P. Configure the ALB's security group to only allow inbound trafficfrom the accelerator's IP addresses on the ALB listener port.

**Answer:** A

**Explanation:**
Please read the below link typically describing ELB integration with AWS Global accelator (and the last line of the extract) - https://docs.aws.amazon.com/global-accelerator/latest/dg/secure-vpc-connections.html "When you add an internal Application Load Balancer or an Amazon EC2 instance endpoint in AWS Global Accelerator, you enable internet traffic to flow directly to and from the endpoint in Virtual Private Clouds (VPCs) by targeting it in a private subnet. The VPC that contains the load balancer or EC2 instance must have an internet gateway attached to it, to indicate that the VPC accepts internet traffic. However, you don't need public IP addresses on the load balancer or EC2 instance. You also don't need an associated internet gateway route for the subnet."

**NEW QUESTION 8**
A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and is hosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolve and connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. The HPC cluster can increase in size by five to seven times during the company’s peak event at the end of the year.
The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries to the default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domain names. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDS and S3 bucket endpoints.
Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VP
B. Reconfigure half of the HPC cluster nodes to use these new DNS server
C. Plan to scale out by adding additional EC2instance-based DNS servers in the future as the HPC cluster size grows.
D. Scale up the existing EC2 instances that the company is using as DNS server
E. Change the instance size to the largest possible instance size to accommodate the current DNS load and theanticipated load in the future.
F. Create Route 53 Resolver outbound endpoint
G. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for on premises hosted domain name
H. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-based DNS server
I. Terminate the EC2 instances.
J. Create Route 53 Resolver inbound endpoint
K. Create rules on the on-premises DNS servers to forward queries to the default VPC resolve
L. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS server
M. Terminate the EC2 instances.

**Answer:** C

**NEW QUESTION 9**
A company is planning to use Amazon S3 to archive financial data. The data is currently stored in an
on-premises data center. The company uses AWS Direct Connect with a Direct Connect gateway and a transit gateway to connect to the on-premises data center. The data cannot be transported over the public internet and must be encrypted in transit.
Which solution will meet these requirements?

A. Create a Direct Connect public VI
B. Set up an IPsec VPN connection over the public VIF to access Amazon S3. Use HTTPS for communication.
C. Create an IPsec VPN connection over the transit VI
D. Create a VPC and attach the VPC to the transit gatewa
E. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication.
F. Create a VPC and attach the VPC to the transit gatewa
G. In the VPC, provision an interface VPC endpoint for Amazon S3. Use HTTPS for communication.

H. Create a Direct Connect public VI
I. Set up an IPsec VPN connection over the public VIF to the transit gatewa
J. Create an attachment for Amazon S3. Use HTTPS for communication.

**Answer:** B

**Explanation:**
https://docs.aws.amazon.com/vpn/latest/s2svpn/private-ip-dx.html
An IPsec VPN connection over the transit VIF can encrypt traffic between the on-premises network and AWS without using public IP addresses or the internet2. A VPC endpoint for Amazon S3 can enable private access to S3 buckets within the same region.HTTPS can provide additional encryption for communication.

**NEW QUESTION 10**
A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple Availability Zones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.
Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The network engineer enables access logging for the ALB.
What should the network engineer do next to determine which errors the ALB is receiving?

A. Send the logs to Amazon CloudWatch Log
B. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB is receiving.
C. Configure the Amazon S3 bucket destinatio
D. Use Amazon Athena to determine which error messages the ALB is receiving.
E. Configure the Amazon S3 bucket destinatio
F. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically, review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.
G. Send the logs to Amazon CloudWatch Log
H. Use the Amazon Athena CloudWatch Connector todetermine which error messages the ALB is receiving.

**Answer:** B

**Explanation:**
Access logs is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logs for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logs at any time.https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

**NEW QUESTION 10**
A company has hundreds of VPCs on AWS. All the VPCs access the public endpoints of Amazon S3 and AWS Systems Manager through NAT gateways. All the traffic from the VPCs to Amazon S3 and Systems Manager travels through the NAT gateways. The company's network engineer must centralize access to these services and must eliminate the need to use public endpoints.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create a central egress VPC that has private NAT gateway
B. Connect all the VPCs to the central egress VPC by using AWS Transit Gatewa
C. Use the private NAT gateways to connect to Amazon S3 and Systems Manager by using private IP addresses.
D. Create a central shared services VP
E. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
F. Ensure that private DNS is turned of
G. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
H. Create an Amazon Route 53 forwarding rule for each interface VPC endpoin
I. Associate the forwarding rules with all the VPC
J. Forward DNS queries to the interface VPC endpoints in the shared services VPC.
K. Create a central shared services VPIn the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
L. Ensure that private DNS is turned of
M. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
N. Create an Amazon Route 53 private hosted zone with a full service endpoint name for Amazon S3 and Systems Manage
O. Associate the private hosted zones with all the VPC
P. Create an alias record in each private hosted zone with the full AWS service endpoint pointing to the interface VPC endpoint in the shared services VPC.
Q. Create a central shared services VP
R. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
S. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
T. Ensure that private DNS is turned on for the interface VPC endpoints and that the transit gateway is created with DNS support turned on.

**Answer:** B

**Explanation:**
Interface VPC endpoints enable private connectivity between VPCs and supported AWS serviceswithout requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection2. Interface VPC endpoints are powered by AWS PrivateLink, a technology that enables private access to AWS services2. Amazon S3 and AWS Systems Manager support interface VPC endpoin2ts. By turning off private DNS, the interface VPC endpoints can be accessed by using their private IP addresses2. By using Amazon Route 53 forwarding rules, DNS queries can be resolved to the interface VPC endpoints in the shared services VPC3.

**NEW QUESTION 11**
A real estate company is building an internal application so that real estate agents can upload photos and videos of various properties. The application will store these photos and videos in an Amazon S3 bucket as objects and will use Amazon DynamoDB to store corresponding metadata. The S3 bucket will be configured to publish all PUT events for new object uploads to an Amazon Simple Queue Service (Amazon SQS) queue.
A compute cluster of Amazon EC2 instances will poll the SQS queue to find out about newly uploaded objects. The cluster will retrieve new objects, perform proprietary image and video recognition and classification update metadata in DynamoDB and replace the objects with new watermarked objects. The company does not want public IP addresses on the EC2 instances.
Which networking design solution will meet these requirements MOST cost-effectively as application usage increases?

A. Place the EC2 instances in a public subne
B. Disable the Auto-assign Public IP option while launching the EC2 instance
C. Create an internet gatewa
D. Attach the internet gateway to the VP
E. In the public subnet's route table, add a default route that points to the internet gateway.
F. Place the EC2 instances in a private subne
G. Create a NAT gateway in a public subnet in the same Availability Zon
H. Create an internet gatewa
I. Attach the internet gateway to the VP
J. In the public subnet's route table, add a default route that points to the internet gateway
K. Place the EC2 instances in a private subne
L. Create an interface VPC endpoint for Amazon SQ
M. Create gateway VPC endpoints for Amazon S3 and DynamoDB.
N. Place the EC2 instances in a private subne
O. Create a gateway VPC endpoint for Amazon SQS.Create interface VPC endpoints for Amazon S3 and DynamoDB.

**Answer:** C

**NEW QUESTION 14**
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.
What are the minimum requirements for your router?

A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
C. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
D. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel

**Answer:** B

**NEW QUESTION 17**
Your company runs an application for the US market in the us-east-1 AWS region. This application uses proprietary TCP and UDP protocols on Amazon Elastic Compute Cloud (EC2) instances. End users run a
real-time, front-end application on their local PCs. This front-end application knows the DNS hostname of the service.
You must prepare the system for global expansion. The end users must access the application with lowest latency.
How should you use AWS services to meet these requirements?

A. Register the IP addresses of the service hosts as “A” records with latency-based routing policy in Amazon Route 53, and set a Route 53 health check for these hosts.
B. Set the Elastic Load Balancing (ELB) load balancer in front of the hosts of the service, and register the ELB name of the main service host as an ALIAS record with a latency-based routing policy in Route 53.
C. Set Amazon CloudFront in front of the host of the service, and register the CloudFront name of the main service as an ALIAS record in Route 53.
D. Set the Amazon API gateway in front of the service, and register the API gateway name of the main service as an ALIAS record in Route 53.

**Answer:** B

**NEW QUESTION 18**
You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.
The instance has a security group configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

The Network ACL for the subnet is configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

When you try to browse to the web server, you receive no response. Which additional step should you take to receive a successful response?

A. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
D. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535

**Answer:** D

**Explanation:**
To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port. The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL.https://aws.amazon.com/premiumsupport/knowledge-center/resolve-connection-sg-acl-inbound/

**NEW QUESTION 20**
A company has expanded its network to the AWS Cloud by using a hybrid architecture with multiple AWS accounts. The company has set up a shared AWS account for the connection to its on-premises data centers and the company offices. The workloads consist of private web-based services for internal use. These services run in different AWS accounts. Office-based employees consume these services by using a DNS name in an on-premises DNS zone that is named example.internal.
The process to register a new service that runs on AWS requires a manual and complicated change request to the internal DNS. The process involves many teams.

The company wants to update the DNS registration process by giving the service creators access that will allow them to register their DNS records. A network engineer must design a solution that will achieve this goal. The solution must maximize cost-effectiveness and must require the least possible number of configuration changes.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.internal). Provide this DNS record to the employees who need access.
B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VP
C. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS server
D. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created.
E. Create an Amazon Route 53 Resolver rule to forward any queries made to onprem.example.internal to the on-premises DNS servers.
F. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWSaccount to resolve queries for this domain.
G. Launch two Amazon EC2 instances in the shared AWS accoun
H. Install BIND on each instanc
I. Create a DNS conditional forwarder on each BIND server to forward queries for each subdomain under aws.example.internal to the appropriate private hosted zone in each AWS accoun
J. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS server
K. Set the forwarding IP addresses to the IP addresses of the BIND servers.
L. Create a private hosted zone in the shared AWS account for each account that runs the service.Configure the private hosted zone to contain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runs the service and the shared account VPC.

**Answer:** ABD

**Explanation:**
To meet the requirements of updating the DNS registration process while maximizing cost-effectiveness and minimizing configuration changes, the network engineer should take the following steps:

- Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint’s IP addresses that were created (Option B).
- Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain (Option D).
- Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.internal). Provide this DNS record to the employees who need access (Option A).

These steps will allow service creators to register their DNS records while keeping costs low and minimizing configuration changes.

**NEW QUESTION 21**
A global delivery company is modernizing its fleet management system. The company has several business units. Each business unit designs and maintains applications that are hosted in its own AWS account in separate application VPCs in the same AWS Region. Each business unit's applications are designed to get data from a central shared services VPC.
The company wants the network connectivity architecture to provide granular security controls. The architecture also must be able to scale as more business units consume data from the central shared services VPC in the future.
Which solution will meet these requirements in the MOST secure manner?

A. Create a central transit gatewa
B. Create a VPC attachment to each application VP
C. Provide full mesh connectivity between all the VPCs by using the transit gateway.
D. Create VPC peering connections between the central shared services VPC and each application VPC in each business unit's AWS account.
E. Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPCCreate VPC endpoints in each application VPC.
F. Create a central transit VPC with a VPN appliance from AWS Marketplac
G. Create a VPN attachment from each VPC to the transit VP
H. Provide full mesh connectivity among all the VPCs.

**Answer:** C

**Explanation:**
Option C provides a secure and scalable solution using VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink enables private connectivity between VPCs and services without exposing the data to the public internet or using a VPN connection. By creating VPC endpoints in each application VPC, the company can securely access the central shared services VPC without the need for complex network configurations. Furthermore, PrivateLink supports cross-account connectivity, which makes it a scalable solution as more business units consume data from the central shared services VPC in the future.

**NEW QUESTION 23**
A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads.
A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time.
How should the network engineer configure routing to meet these requirements?

A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual applianc
B. Add routes that are more specific to point to the primary SD-WAN virtual appliance.
C. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.
D. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway.
E. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

**Answer:** A

**NEW QUESTION 25**
A company is using Amazon Route 53 Resolver DNS Firewall in a VPC to block all domains except domains that are on an approved list. The company is concerned that if DNS Firewall is unresponsive, resources in the VPC might be affected if the network cannot resolve any DNS queries. To maintain application service level agreements, the company needs DNS queries to continue to resolve even if Route 53 Resolver does not receive a response from DNS Firewall.
Which change should a network engineer implement to meet these requirements?

A. Update the DNS Firewall VPC configuration to disable fail open for the VPC.
B. Update the DNS Firewall VPC configuration to enable fail open for the VPC.
C. Create a new DHCP options set with parameter dns_firewall_fail_open=fals
D. Associate the new DHCP options set with the VPC.
E. Create a new DHCP options set with parameter dns_firewall_fail_open=tru
F. Associate the new DHCP options set with the VPC.

**Answer:** B

**NEW QUESTION 29**
A company has created three VPCs: a production VPC, a nonproduction VPC, and a shared services VPC. The production VPC and the nonproduction VPC must each have communication with the shared services VPC. There must be no communication between the production VPC and the nonproduction VPC. A transit gateway is deployed to facilitate communication between VPCs.
Which route table configurations on the transit gateway will meet these requirements?

A. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for only the shared services VP
B. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
C. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for each VP
D. Create an additional route table with only the shared services VPC attachment associated with propagated routes from each VPC.
E. Configure a route table with all the VPC attachments associated with propagated routes for only the shared services VPCreate an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
F. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes disable
G. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

**Answer:** A

**NEW QUESTION 33**
A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2 Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.
A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediates noncompliant changes to security groups.
Which solution will meet these requirements?

A. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuratio
B. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.
C. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuratio
D. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.
E. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security group configuratio
F. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.
G. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuratio
H. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

**Answer:** D

**Explanation:**
Configuring an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security group configuration would enable evaluation of the compliance status of the security groups based on predefined or custom rules3. Creating an AWS Systems Manager Automation runbook to remediate noncompliant security groups would enable automation of the remediation process2. Additionally, configuring AWS Config to trigger the runbook when a noncompliant change is detected would enable timely and consistent remediation of security group changes.

**NEW QUESTION 34**
A company hosts an application on Amazon EC2 instances behind an Application Load Balancer (ALB). The company recently experienced a network security breach. A network engineer must collect and analyze logs that include the client IP address, target IP address, target port, and user agent of each user that accesses the application.
What is the MOST operationally efficient solution that meets these requirements?

A. Configure the ALB to store logs in an Amazon S3 bucke
B. Download the files from Amazon S3, and use a spreadsheet application to analyze the logs.
C. Configure the ALB to push logs to Amazon Kinesis Data Stream
D. Use Amazon Kinesis Data Analytics to analyze the logs.
E. Configure Amazon Kinesis Data Streams to stream data from the ALB to Amazon OpenSearch Service (Amazon Elasticsearch Service). Use search operations in Amazon OpenSearch Service (Amazon Elasticsearch Service) to analyze the data.
F. Configure the ALB to store logs in an Amazon S3 bucke
G. Use Amazon Athena to analyze the logs in Amazon S3.

**Answer:** D

**Explanation:**
The most operationally efficient solution to collect and analyze logs that include the client IP address, target IP address, target port, and user agent of each user that accesses the application would be to configure the ALB to store logs in an Amazon S3 bucket and use Amazon Athena to analyze the logs in Amazon S3 (Option D). This solution allows for quick and easy analysis of log data without requiring manual download or manipulation of log files.

**NEW QUESTION 37**
A company has deployed an AWS Network Firewall firewall into a VPC. A network engineer needs to implement a solution to deliver Network Firewall flow logs to the company's Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster in the shortest possible time.
Which solution will meet these requirements?

A. Create an Amazon S3 bucke
B. Create an AWS Lambda function to load logs into the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluste

C. Enable Amazon Simple Notification Service (Amazon SNS) notifications on the S3 bucket to invoke the Lambda functio
D. Configure flow logs for the firewal
E. Set the S3 bucket as the destination.
F. Create an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destinatio
G. Configure flow logs for the firewall Set the Kinesis Data Firehose delivery stream as the destination for the Network Firewall flow logs.
H. Configure flow logs for the firewal
I. Set the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination for the Network Firewall flow logs.
J. Create an Amazon Kinesis data stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destinatio
K. Configure flow logs for the firewal
L. Set the Kinesis data stream as the destination for the Network Firewall flow logs.

**Answer:** B

**Explanation:**
https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-analyze-aws-network-firewall-logs-usin

**NEW QUESTION 40**
A global company operates all its non-production environments out of three AWS Regions: eu-west-1,
us-east-1, and us-west-1. The company hosts all its production workloads in two on-premises data centers. The company has 60 AWS accounts and each account has two VPCs in each Region. Each VPC has a virtual private gateway where two VPN connections terminate for resilient connectivity to the data centers. The company has 360 VPN tunnels to each data center, resulting in high management overhead. The total VPN throughput for each Region is 500 Mbps.
The company wants to migrate the production environments to AWS. The company needs a solution that will simplify the network architecture and allow for future growth. The production environments will generate an additional 2 Gbps of traffic per Region back to the data centers. This traffic will increase over time.
Which solution will meet these requirements?

A. Set up an AWS Direct Connect connection from each data center to AWS in each Regio
B. Create and attach private VIFs to a single Direct Connect gatewa
C. Attach the Direct Connect gateway to all the VPC
D. Remove the existing VPN connections that are attached directly to the virtual private gateways.
E. Create a single transit gateway with VPN connections from each data cente
F. Share the transit gateway with each account by using AWS Resource Access Manager (AWS RAM). Attach the transit gateway to each VP
G. Remove the existing VPN connections that are attached directly to the virtual private gateways.
H. Create a transit gateway in each Region with multiple newly commissioned VPN connections from each data cente
I. Share the transit gateways with each account by using AWS Resource Access Manager (AWS RAM). In each Region, attach the transit gateway to each VPRemove the existing VPN connections that are attached directly to the virtual private gateways.
J. Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VP
K. Create new VPN connections from each data center to the transit VPC
L. Terminate the original VPN connections that are attached to all the original VPC
M. Retain the new VPN connection to the new transit VPC in each Region.

**Answer:** C

**NEW QUESTION 44**
A company has a hybrid cloud environment. The company’s data center is connected to the AWS Cloud by an AWS Direct Connect connection. The AWS environment includes VPCs that are connected together in a hub-and-spoke model by a transit gateway. The AWS environment has a transit VIF with a Direct Connect gateway for on-premises connectivity.
The company has a hybrid DNS model. The company has configured Amazon Route 53 Resolver endpoints in the hub VPC to allow bidirectional DNS traffic flow. The company is running a backend application in one of the VPCs.
The company uses a message-oriented architecture and employs Amazon Simple Queue Service (Amazon SQS) to receive messages from other applications over a private network. A network engineer wants to use an interface VPC endpoint for Amazon SQS for this architecture. Client services must be able to access the endpoint service from on premises and from multiple VPCs within the company's AWS infrastructure.
Which combination of steps should the network engineer take to ensure that the client applications can resolve DNS for the interface endpoint? (Choose three.)

A. Create the interface endpoint for Amazon SQS with the option for private DNS names turned on.
B. Create the interface endpoint for Amazon SQS with the option for private DNS names turned off.
C. Manually create a private hosted zone for sqs.us-east-1.amazonaws.co
D. Add necessary records that point to the interface endpoin
E. Associate the private hosted zones with other VPCs.
F. Use the automatically created private hosted zone for sqs.us-east-1.amazonaws.com with previously created necessary records that point to the interface endpoin
G. Associate the private hosted zones with other VPCs.
H. Access the SQS endpoint by using the public DNS name sqs.us-east-1 amazonaws.com in VPCs and on premises.
I. Access the SQS endpoint by using the private DNS name of the interface endpoint.sqs.us-east-1.vpce.amazonaws.com in VPCs and on premises.

**Answer:** ADF

**NEW QUESTION 45**
A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application must always be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change to the EC2 security group.
A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever a change is made to the security group. The solution also must notify the network engineer when the change affects the connection.
Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Log
B. Create a CloudWatch Logs metric filter for the log group for rejected traffi
C. Create an alarm to notify the network engineer.
D. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Log

E. Create a CloudWatch Logs metric filter for the log group for all traffi
F. Create an alarm to notify the network engineer
G. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the sourc
H. Specify the EC2 instances as the destinatio
I. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connectio
J. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security groupoccurs.
K. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the sourc
L. Specify the EC2 instances as the destinatio
M. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connectio
N. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fai
O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs.

**Answer:** C

**NEW QUESTION 46**
A company has a global network and is using transit gateways to connect AWS Regions together. The company finds that two Amazon EC2 instances in different Regions are unable to communicate with each other. A network engineer needs to troubleshoot this connectivity issue.
What should the network engineer do to meet this requirement?

A. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables and in the VPC route table
B. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.
C. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables.Verify that the VPC route tables are correc
D. Use AWS Firewall Manager to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.
E. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables.Verify that the VPC route tables are correc
F. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.
G. Use VPC Reachability Analyzer to analyze routes in the transit gateway route table
H. Verify that the VPC route tables are correc
I. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

**Answer:** C

**Explanation:**
Using AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables would enable identification of routing issues between VPCs and transit gateways1. Verifying that the VPC route tables are correct would enable identification of routing issues within a VPC. Using VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC would enable identification of traffic filtering issues within a VPC2. Additionally, using VPC Reachability Analyzer to analyze routes in the transit gateway route tables would enable identification of routing issues between transit gateways in different Regions. VPC Reachability Analyzer is a configuration analysis tool that enables connectivity testing between a source resource and a destination resource in your VPCs.

**NEW QUESTION 49**
A software company offers a software-as-a-service (SaaS) accounting application that is hosted in the AWS Cloud The application requires connectivity to the company's on-premises network. The company has two redundant 10 GB AWS Direct Connect connections between AWS and its on-premises network to accommodate the growing demand for the application.
The company already has encryption between its on-premises network and the colocation. The company needs to encrypt traffic between AWS and the edge routers in the colocation within the next few months. The company must maintain its current bandwidth.
What should a network engineer do to meet these requirements with the LEAST operational overhead?

A. Deploy a new public VIF with encryption on the existing Direct Connect connection
B. Reroute traffic through the new public VIF.
C. Create a virtual private gateway Deploy new AWS Site-to-Site VPN connections from on premises to the virtual private gateway Reroute traffic from the Direct Connect private VIF to the new VPNs.
D. Deploy a new pair of 10 GB Direct Connect connections with MACse
E. Configure MACsec on the edge router
F. Reroute traffic to the new Direct Connect connection
G. Decommission the original Direct Connect connections
H. Deploy a new pair of 10 GB Direct Connect connections with MACse
I. Deploy a new public VIF on the new Direct Connect connection
J. Deploy two AWS Site-to-Site VPN connections on top of the new public VI
K. Reroute traffic from the existing private VIF to the new Site-to-Site connection
L. Decommission the original Direct Connect connections.

**Answer:** C

**NEW QUESTION 52**
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.
Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: “There are not enough free addresses in subnet ‘subnet-12345677’ to satisfy the requested number of instances.”
What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CID
B. Include the new subnet in the Auto Scaling group.
C. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CID
D. Include the new subnet in the Auto Scaling group.
E. Resize the IPv6 CIDR on each of the existing subnet
F. Modify the Auto Scaling group maximum number of instances.
G. Add a secondary IPv4 CIDR to the Amazon VP
H. Assign secondary IPv4 address space to each of theexisting subnets.

**Answer:** B

**NEW QUESTION 57**
A banking company is successfully operating its public mobile banking stack on AWS. The mobile banking stack is deployed in a VPC that includes private subnets and public subnets. The company is using IPv4 networking and has not deployed or supported IPv6 in the environment. The company has decided to adopt a third-party service provider's API and must integrate the API with the existing environment. The service provider's API requires the use of IPv6.
A network engineer must turn on IPv6 connectivity for the existing workload that is deployed in a private subnet. The company does not want to permit IPv6 traffic from the public internet and mandates that the company's servers must initiate all IPv6 connectivity. The network engineer turns on IPv6 in the VPC and in the private subnets.
Which solution will meet these requirements?

A. Create an internet gateway and a NAT gateway in the VP
B. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT gateway.
C. Create an internet gateway and a NAT instance in the VP
D. Add a route to the existing subnet route tables to point IPv6 traffic to the NAT instance.
E. Create an egress-only Internet gateway in the VPAdd a route to the existing subnet route tables topoint IPv6 traffic to the egress-only internet gateway.
F. Create an egress-only internet gateway in the VP
G. Configure a security group that denies all inbound traffi
H. Associate the security group with the egress-only internet gateway.

**Answer:** C

**NEW QUESTION 60**
A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin in an Amazon CloudFront distribution. The company wants to implement a custom authentication system that will provide a token for its authenticated customers.
The web application must ensure that the GET/POST requests come from authenticated customers before it delivers the content. A network engineer must design a solution that gives the web application the ability to identify authorized customers.
What is the MOST operationally efficient solution that meets these requirements?

A. Use the ALB to inspect the authorized token inside the GET/POST request payloa
B. Use an AWS Lambda function to insert a customized header to inform the web application of an authenticated customer request.
C. Integrate AWS WAF with the ALB to inspect the authorized token inside the GET/POST request payloa
D. Configure the ALB listener to insert a customized header to inform the web application of an authenticated customer request.
E. Use an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payloa
F. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request.
G. Set up an EC2 instance that has a third-party packet inspection tool to inspect the authorized token inside the GET/POST request payloa
H. Configure the tool to insert a customized header to inform the web application of an authenticated customer request.

**Answer:** C

**NEW QUESTION 62**
A company is deploying a new application in the AWS Cloud. The company wants a highly available web server that will sit behind an Elastic Load Balancer. The load balancer will route requests to multiple target groups based on the URL in the request. All traffic must use HTTPS. TLS processing must be offloaded to the load balancer. The web server must know the user's IP address so that the company can keep accurate logs for security purposes.
Which solution will meet these requirements?

A. Deploy an Application Load Balancer with an HTTPS listene
B. Use path-based routing rules to forward the traffic to the correct target grou
C. Include the X-Forwarded-For request header with traffic to the targets.
D. Deploy an Application Load Balancer with an HTTPS listener for each domai
E. Use host-based routing rules to forward the traffic to the correct target group for each domai
F. Include the X-Forwarded-For request header with traffic to the targets.
G. Deploy a Network Load Balancer with a TLS listene
H. Use path-based routing rules to forward the traffic to the correct target grou
I. Configure client IP address preservation for traffic to the targets.
J. Deploy a Network Load Balancer with a TLS listener for each domai
K. Use host-based routing rules to forward the traffic to the correct target group for each domai
L. Configure client IP address preservation for traffic to the targets.

**Answer:** A

**Explanation:**
An Application Load Balancer (ALB) can be used to route traffic to multiple target groups based on the URL in the request. The ALB can be configured with an HTTPS listener to ensure all traffic uses HTTPS. TLS processing can be offloaded to the ALB, which reduces the load on the web server. Path-based routing rules can be used to route traffic to the correct target group based on the URL in the request. The X-Forwarded-For request header can be included with traffic to the targets, which will allow the web server to know the user's IP address and keep accurate logs for security purposes.

**NEW QUESTION 66**
A company's network engineer needs to design a new solution to help troubleshoot and detect network anomalies. The network engineer has configured Traffic Mirroring. However, the mirrored traffic is overwhelming the Amazon EC2 instance that is the traffic mirror target. The EC2 instance hosts tools that the company's security team uses to analyze the traffic. The network engineer needs to design a highly available solution that can scale to meet the demand of the mirrored traffic.
Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) as the traffic mirror targe
B. Behind the NL
C. deploy a fleet of EC2 instances in an Auto Scaling grou
D. Use Traffic Mirroring as necessary.
E. Deploy an Application Load Balancer (ALB) as the traffic mirror targe

F. Behind the ALB, deploy a fleet of EC2 instances in an Auto Scaling grou
G. Use Traffic Mirroring only during non-business hours.
H. Deploy a Gateway Load Balancer (GLB) as the traffic mirror targe
I. Behind the GL
J. deploy a fleet of EC2 instances in an Auto Scaling grou
K. Use Traffic Mirroring as necessary.
L. Deploy an Application Load Balancer (ALB) with an HTTPS listener as the traffic mirror targe
M. Behind the AL
N. deploy a fleet of EC2 instances in an Auto Scaling grou
O. Use Traffic Mirroring only during active events or business hours.

**Answer:** A

**NEW QUESTION 68**
A bank built a new version of its banking application in AWS using containers that content to an on-premises database over VPN connection. This application version requires users to also update their client application. The bank plans to deprecate the earlier client version. However, the company wants to keep supporting earlier clients through their on-premises version of the application to serve a small portion of the customers who haven't yet upgraded.
What design will allow the company to serve both newer and earlier clients in the MOST efficient way?

A. Use an Amazon Route 53 multivalue answer routing policy to route older client traffic to the on-premises application version and the rest of the traffic to the new AWS based version.
B. Use a Classic Load Balancer for the new applicatio
C. Route all traffic to the new application by using an Elastic Load Balancing (ELB) load balancer DN
D. Define a user-agent-based rule on the backend servers to redirect earlier clients to the on-premises application.
E. Use an Application Load Balancer for the new applicatio
F. Register both the new and earlier applications as separate target groups and use path-based routing to route traffic based on the application version.
G. Use an Application Load Balancer for the new applicatio
H. Register both the new and earlier application backends as separate target group
I. Use header-based routing to route traffic based on the application version.

**Answer:** D

**NEW QUESTION 69**
An organization is replacing a tape backup system with a storage gateway. there is currently no connectivity to AWS. Initial testing is needed.
What connection option should the organization use to get up and running at minimal cost?

A. Use an internet connection.
B. Set up an AWS VPN connection.
C. Provision an AWS Direct Connection private virtual interface.
D. Provision a Direct Connect public virtual interface.

**Answer:** A

**NEW QUESTION 74**
A company is deploying a new application on AWS. The application uses dynamic multicasting. The company has five VPCs that are all attached to a transit gateway Amazon EC2 instances in each VPC need to be able to register dynamically to receive a multicast transmission.
How should a network engineer configure the AWS resources to meet these requirements?

A. Create a static source multicast domain within the transit gatewa
B. Associate the VPCs and applicable subnets with the multicast domai
C. Register the multicast senders' network interface with the multicast domai
D. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.
E. Create a static source multicast domain within the transit gatewa
F. Associate the VPCs and applicable subnets with the multicast domai
G. Register the multicast senders' network interface with the multicast domai
H. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.
I. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway.Associate the VPCs and applicable subnets with the multicast domai
J. Register the multicast senders' network interface with the multicast domai
K. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.
L. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway.Associate the VPCs and applicable subnets with the multicast domai
M. Register the multicast senders' network interface with the multicast domai
N. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

**Answer:** C

**NEW QUESTION 79**
A company's AWS architecture consists of several VPCs. The VPCs include a shared services VPC and several application VPCs. The company has established network connectivity from all VPCs to the
on-premises DNS servers.
Applications that are deployed in the application VPCs must be able to resolve DNS for internally hosted domains on premises. The applications also must be able to resolve local VPC domain names and domains that are hosted in Amazon Route 53 private hosted zones.
What should a network engineer do to meet these requirements?

A. Create a new Route 53 Resolver inbound endpoint in the shared services VP
B. Create forwarding rules for the on-premises hosted domain
C. Associate the rules with the new Resolver endpoint and each application VP
D. Update each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.

E. Create a new Route 53 Resolver outbound endpoint in the shared services VP
F. Create forwarding rules for the on-premises hosted domain
G. Associate the rules with the new Resolver endpoint and each application VPC.
H. Create a new Route 53 Resolver outbound endpoint in the shared services VPCreate forwarding rules for the on-premises hosted domain
I. Associate the rules with the new Resolver endpoint and each application VPUpdate each application VPC's DHCP configuration to point DNS resolution to the new Resolver endpoint.
J. Create a new Route 53 Resolver inbound endpoint in the shared services VP
K. Create forwarding rules for the on-premises hosted domain
L. Associate the rules with the new Resolver endpoint and each application VPC.

**Answer:** B

**Explanation:**
Creating a new Route 53 Resolver outbound endpoint in the shared services VPC would enable forwarding of DNS queries from the VPC to on-premises1. Creating forwarding rules for the on-premises hosted domains would enable specifying which domain names are forwarded to the on-premises DNS servers2. Associating the rules with the new Resolver endpoint and each application VPC would enable applying the rules to the VPCs2. This solution would not affect the default DNS resolution behavior of Route 53 Resolver for local VPC domain names and domains that are hosted in Route 53 private hosted zones3.

**NEW QUESTION 84**
A company recently migrated its Amazon EC2 instances to VPC private subnets to satisfy a security compliance requirement. The EC2 instances now use a NAT gateway for internet access. After the migration, some long-running database queries from private EC2 instances to a publicly accessible third-party database no longer receive responses. The database query logs reveal that the queries successfully completed after 7 minutes but that the client EC2 instances never received the response.
Which configuration change should a network engineer implement to resolve this issue?

A. Configure the NAT gateway timeout to allow connections for up to 600 seconds.
B. Enable enhanced networking on the client EC2 instances.
C. Enable TCP keepalive on the client EC2 instances with a value of less than 300 seconds.
D. Close idle TCP connections through the NAT gateway.

**Answer:** C

**Explanation:**
When a TCP connection is idle for a long time, it may be terminated by network devices, including the NAT gateway. By enabling TCP keepalive, the client EC2 instances can periodically send packets to the third-party database to indicate that the connection is still active, preventing it from being terminated prematurely.

**NEW QUESTION 87**
A company uses AWS Direct Connect to connect its corporate network to multiple VPCs in the same AWS account and the same AWS Region. Each VPC uses its own private VIF and its own virtual LAN on the Direct Connect connection. The company has grown and will soon surpass the limit of VPCs and private VIFs for each connection.
What is the MOST scalable way to add VPCs with on-premises connectivity?

A. Provision a new Direct Connect connection to handle the additional VPC
B. Use the new connection to connect additional VPCs.
C. Create virtual private gateways for each VPC that is over the service quot
D. Use AWS Site-to-Site VPNto connect the virtual private gateways to the corporate network.
E. Create a Direct Connect gateway, and add virtual private gateway associations to the VPC
F. Configure a private VIF to connect to the corporate network.
G. Create a transit gateway, and attach the VPC
H. Create a Direct Connect gateway, and associate it with the transit gatewa
I. Create a transit VIF to the Direct Connect gateway.

**Answer:** D

**Explanation:**
When a company requires connectivity to multiple VPCs over AWS Direct Connect, a scalable solution is to use a transit gateway. A transit gateway is a hub that can interconnect multiple VPCs and VPN connections. The VPCs can communicate with each other over the transitgateway, and on-premises networks can communicate with the VPCs through the Direct Connect gateway. This solution provides a central point of management and simplifies the configuration of network routing. By associating the Direct Connect gateway with the transit gateway, traffic between the VPCs and the on-premises network can be routed through the Direct Connect connection.

**NEW QUESTION 89**
......