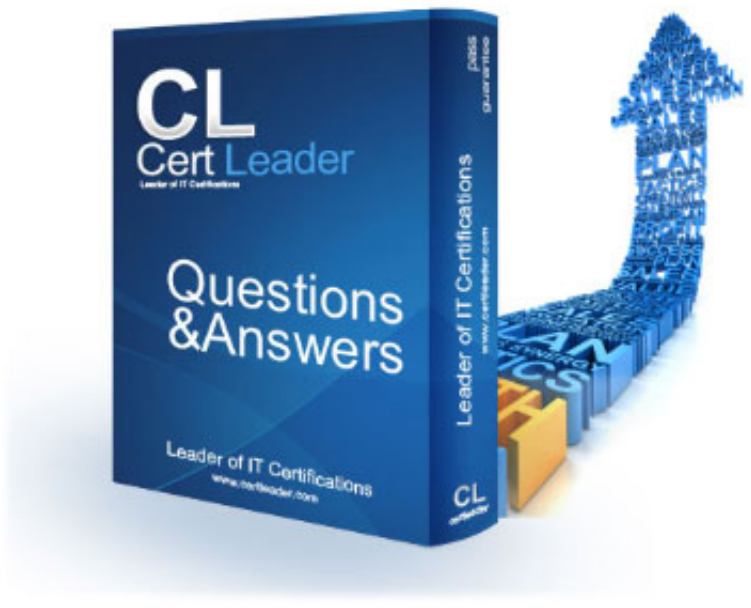
AWS-Certified-Advanced-Networking-Specialty Dumps

Amazon AWS Certified Advanced Networking - Specialty

https://www.certleader.com/AWS-Certified-Advanced-Networking-Specialty-dumps.html



NEW QUESTION 1
A company has an application running on Amazon EC2 instances in a VPC The application must publish custom metrics to Amazon CloudWatch in the same AWS Region The metrics include proprietary information All connectivity must be over private IP addresses.
Which solution will meet these requirements'?

A. Connect to CloudWatch through a NAT gateway
B. Connect to CloudWatch through a gateway endpoint
C. Connect to CloudWatch through an internet gateway
D. Connect to CloudWatch through an interface endpoint

Answer: D

NEW QUESTION 2
A logistics company has deployed a hybrid environment that has multiple VPCs in both the us-east-1 Region and the af-south-1 Region The on-premises data center is connected to us-east-1 through an AWS Direct Connect connection The Direct Connect connection is connected to a Direct Connect gateway that is associated with a transit gateway The transit gateway is attached to all the VPCs in us-east-1
An application that is deployed in af-south-1 requires access to a database in the data center The application also requires access to file storage in a VPC in us-east-1
Which solution will meet these requirements with the LOWEST latency?

A. Create a transit gateway in af-south-1, and attach the VPCs Create a transit gateway peering connection between the transit gateways
B. Create a Direct Connect connection in af-south-1, and attach the VPCs with a Direct Connect gateway and a transit gateway Create an AWS Site-to-Site VPN connection over the internet between the Direct Connect connections.
C. Create a transit gateway in af-south-1 and attach the VPCs Associate the transit gateway in af-south-1 with the Direct Connect gateway tn us-east-1
D. Create inter-Region VPC peering connections between the VPCs in each Region Use the transit gateway attachments in us-east-1 to access the database in the data center

Answer: A

NEW QUESTION 3
A company hosts several applications in the AWS Cloud across multiple VPCs that are connected to a transit gateway Redundant AWS Direct Connect connections and a Direct Connect gateway provide private network connectivity lo the company's on-premises environment
During a maintenance window, the networking team adds eight VPCs The application management team notices that there is no reachability between the newly created VPCs and the on-premises environment Connectivity between all VPCs through the transit gateway is working as expected.
Which of the following are possible causes of the connectivity issues? (Choose TWO)

A. The prefixes that are advertised from the Direct Connect gateway to the on-premises router are shorter than the CIDR blocks of the newly created VPCs
B. The route tables for the newly created
C. VPCs do not have the routes to the on-premises environment that point to the transit gateway attachment
D. The on-premises route tables do not contain the exact CIDR blocks of the newly created VPCs
E. The route tables (or the newly created VPCs have only summary routes for (he on-premises environment (fiat point to the transit gateway attachment.
F. The prefixes that are advertised from the Direct Connect gateway to the on-premises router do not contain the CIDR blocks of the newly created VPCs

Answer: AD

NEW QUESTION 4
A company is deploying a non-web application on an AWS load balancer. All targets are servers located
on-premises that can be accessed by using AWS Direct Connect. The company wants to ensure that the source IP addresses of clients connecting to the application are passed all the way to the end server.
How can this requirement be achieved?

A. Use a Network Load Balancer to automatically preserve the source IP address.
B. Use a Network Load Balancer and enable the X-Forwarded-For attribute.
C. Use a Network Load Balancer and enable the ProxyProtocol v2 attribute.
D. Use an Application Load Balancer to automatically preserve the source IP address in the X-Forwarded-For header.

Answer: C

Explanation:
https://docs.aws.amazon.com/elasticloadbalancing/latest/network/load-balancer-target-groups.html#proxy-proto

NEW QUESTION 5
A company wants to migrate its workloads to the AWS Cloud. The company has two web applications and wants to run them in separate, isolated VPCs. The company needs to use Elastic Load Balancing to distribute requests between application instances.
For security reasons, internet gateways must not be attached to the application VPCs. Inbound HTTP requests to the application must be routed through a centralized VPC. and the application VPCs must not be exposed to any other inbound traffic The application VPCs cannot be allowed to initiate any outbound connections
What should a network engineer do to meet these requirements?

A. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
B. Create a public Network Load Balancer (NLB) in the centralized VP
C. Create target groups for the private DNS names of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.
D. Run the applications behind private Application Load Balancers (ALBs) in separate VPC
E. Create a public Network Load Balancer (NLB) in the centralized VP
F. Create target groups for the private IP addresses of the ALBs Configure host-based routing to route application traffic to the corresponding target group through the NLB.

G. Run the applications behind private Network Load Balancers (NLBs) in separate VPC
H. Create VPC peering connections between the application VPCs and the centralized VP
I. Create a public Application Load Balancer (ALB) in the centralized VP
J. Create target groups for the private DNS names of the NLB
K. Configure host-based routing to route application traffic between individual applications though the ALB.
L. Run the applications behind private Network Load Balancers (NLBs) inseparate VPC
M. Configure each NLB as an AWS PrivateLink endpoint service with associated VPC endpoints in the centralized VPC Create target groups that include the private IP addresses of each endpoin
N. Create a public Application Load Balancer (ALB) in the centralized VP
O. Configurehost-based routing to route application traffic to the corresponding target group through the ALB.

Answer: D

NEW QUESTION 6
Your organization runs a popular e-commerce application deployed on AWS that uses autoscaling in conjunction with an Elastic Load balancing (ELB) service with an HTTPS listener. Your security team reports that an exploitable vulnerability has been discovered in the encryption protocol and cipher that your site uses.
Which step should you take to fix this problem?

A. Generate new SSL certificates for all web servers and replace current certificates.
B. Change the security policy on the ELB to disable vulnerable protocols and ciphers.
C. Generate new SSL certificates and use ELB to front-end the encrypted traffic for all web servers.
D. Leverage your current configuration management system to update SSL policy on all web servers.

Answer: B

NEW QUESTION 7
Your company decides to use Amazon S3 to augment its on-premises data store. Instead of using the company's highly controlled, on-premises Internet gateway, a Direct Connect connection is ordered to provide high bandwidth, low latency access to S3. Since the company does not own a publically routable IPv4 address block, a request was made to AWS for an AWS-owned address for a Public Virtual Interface (VIF).
The security team is calling this new connection a "backdoor", and you have been asked to clarify the risk to the company.
Which concern from the security team is valid and should be addressed?

A. AWS advertises its aggregate routes to the Internet allowing anyone on the Internet to reach the router.
B. Direct Connect customers with a Public VIF in the same region could directly reach the router.
C. EC2 instances in the same region with access to the Internet could directly reach the router.
D. The S3 service could reach the router through a pre-configured VPC Endpoint.

Answer: C

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/control-routes-direct-connect/

NEW QUESTION 8
A company uses AWS Direct Connect lo connect its corporate network to multiple VPCs in the same AWS account and the same AVVS 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 VPCs Use the new connection to connect additional VPCs.
B. Create virtual private gateways for each VPC that is over the service quota Use AWS Site-to-Site VPN to connect the virtual private gateways to the corporate network
C. Create a Direct Connect gateway, and add virtual private gateway associations to the VPC
D. Configure a private VIF to connect to the corporate network
E. Create a transit gateway and attach the VPCs Create a Direct Connect gateway, and associate it with the transit gateway Create a transit VIF to the Direct Connect gateway

Answer: D

NEW QUESTION 9
A company with several VPCs in the us-east-1 Region wants to reduce the cost of its workloads A network engineer has identified that all traffic bound to Amazon services is flowing through a NAT gateway. Additionally, all the VPCs are peered to a hub VPC for access to common services.

A. Disable the private DNS name for the SQS endpoin
B. Create an Amazon Route 53 private hosted zone for the domain us-east-1.sqs.amazonaws.co
C. Create a CNAME record to the DNS name of the SQS endpoint Share the private hosted zone with ail other VPCs
D. Disable the private DNS name for the SOS endpoin
E. Create an Amazon Route 53 private hosted zone for the domain sqs.us-east-1 .amazonaws.co
F. Create an alias record to the DNS name of the SOS endpoin
G. Share the private hosted zone with all other VPCs
H. Enable the private DNS name for the SOS endpoint Create an Amazon Route 53 private hosted zone for the domain SQS.us-east-t.amazonaws.co
I. Create a CNAME record to the DNS name of the SQS endpoin
J. Share the private hosted zone with all other VPCs.
K. Enable the private DNS name for the SQS endpoin
L. Create an Amazon Route 53 private hosted zone for the domain us-east-1 .sqs.amazonaws.co
M. Create an alias record to the DNS name of the SQS endpoin
N. Share the private hosted zone with all other VPCs.

Answer: A

NEW QUESTION 10
Your company needs to leverage Amazon Simple Storage Solution (S3) for backup and archiving. According to company policy, data should not flow on the public Internet even if data is encrypted. You have set up two S3 buckets in us-east-1 and us-west-2. Your company data center is located on the West Coast of the United States. The design must be cost-effective and enable minimal latency.
Which design should you set up?

A. An AWS Direct Connect connection to us-east-1 and a Direct Connect connection to us-west-2.
B. An AWS Direct Connect connection to us-east-1.
C. An AWS Direct Connect connection to us-west-2.
D. An AWS Direct Connect connection to us-west-2 and a VPN connection to us-east-1.

Answer: C

NEW QUESTION 10
A company's web application is deployed on Amazon EC2 instances behind a public Application Load Balancer. The application flags malicious requests and uses an AWS Lambda function to add the offending IP addresses to the network ACL to block any further request for 24 hours. Recently, the application has been receiving more malicious requests, which causes the network ACL to reach its limit of allowed entries.
Which action should be taken to block more IP addresses, without compromising the existing security requirements?

A. Update the AWS Lambda function to remove blocked entries from the network ACL after 2 hours.
B. Update the AWS Lambda function to block malicious IPs in security groups rather than the network ACL.
C. Update the AWS Lambda function to block malicious IPs in AWS WAF attached to the Application Load Balancer.
D. Update the AWS Lambda function to add an additional network ACL to the subnets once the limit for the previous ones has been reached.

Answer: C

NEW QUESTION 14
A department in your company has created a new account that is not part of the organization's consolidated billing family. The department has also created a VPC for its workload. Access is restricted by network access control lists to the department's on-premises private IP allocation. An AWS Direct Connect private virtual interface for this VPC advertises a default route to the company network. When the department downloads data from an Amazon Elastic Compute Cloud(EC2) instance in its new VPC, what are the associated charges?

A. The company pays Internet Data Out charges.
B. The company pays AWS Direct Connect Data Out charges.
C. The department pays Internet Data Out charges.
D. The department pays AWS Direct Connect Data Out charges.

Answer: D

NEW QUESTION 16
A company provisions an AWS Direct Connect connection to permit access to Amazon EC2 resources in several Amazon VPCs and to data stored in private Amazon S3 buckets. The Network Engineer needs to configure the company's on-premises router for this Direct Connect connection.
Which of the following actions will require the LEAST amount of configuration overhead on the customer router?

A. Configure private virtual interfaces for the VPC resources and for Amazon S3.
B. Configure private virtual interfaces for the VPC resources and a public virtual interface for Amazon S3.
C. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and for Amazon S3.
D. Configure a private virtual interface to a Direct Connect gateway for the VPC resources and a public virtual interface for Amazon S3.

Answer: A

NEW QUESTION 21
You have multiple Amazon Elastic Compute Cloud (EC2) instances running a web server in a VPC configured with security groups and NACL. You need to ensure layer 7 protocol level logging of all network traffic (ACCEPT/REJECT) on the instances. What should be enabled to complete this task?

A. CloudWatch Logs at the VPC level
B. Packet sniffing at the instance level
C. VPC flow logs at the subnet level
D. Packet sniffing at the VPC level

Answer: B

NEW QUESTION 26
An architecture is being designed to support an Amazon WorkSpaces deployment of 1,000 desktops. Which architecture will support this deployment while allowing for future expansion?

A. A VPC with a /16 CIDR and one /21 subnet
B. A VPC with a /20 CIDR and two /21 subnets
C. A VPC with a /16 CIDR and one /22 subnet
D. A VPC with a /20 CIDR and two /23 subnets

Answer: B

NEW QUESTION 31
A company has Iwo on-premises data center locations. There is a company-managed router at earn data center. Each data center has a dedicated AWS Direct Connect connection to a Direct Connect gateway through a private virtual interface The router for the first location is advertising 110 routes to the Direct Connect gateway by using BGP and the router tor the second location is advertising 60 routes to the Direct Connect gateway by using BGP The Direct Connect gateway is

attached to a company VPC through a virtual private gateway
A network engineer receives reports that resources In the VPC are not reachable from various locations in either data center. The network engineer checks the VPC route table and sees that the routes from the first data center. location are not being populated into the route table The network engineer must resolve this issue in the most operationally efficient manner
What should the network engineer do to meet these requirements'

A. Remove the Direct Connect gateway, and create a new private virtual interface from each company router to the virtual private gateway of the VPC
B. Change the router configurations to summarize the advertised routes
C. Open a support ticket to increase the quota on advertised routes to the VPC route table
D. Create an AWS Transit Gateway Attach the transit gateway to the VPC and connect the Direct Connect gateway to the transit gateway.

Answer: D

NEW QUESTION 33
Your company runs an HTTPS application using an Elastic Load Balancing (ELB) load balancer/PHP on nginx server/RDS in multiple Availability Zones. You need to apply Geographic Restriction and identify the client's IP address in your application to generate dynamic content.
How should you utilize AWS services in a scalable fashion to perform this task?

A. Modify the nginx log configuration to record value in X-Forwarded-For and use CloudFront to apply the Geographic Restriction.
B. Enable ELB access logs to store the client IP address and parse these to dynamically modify a blacklist.
C. Use X-Forwarded-For with security groups to apply the Geographic Restriction.
D. Modify the application code to use value of X-Forwarded-For and CloudFront to apply the Geographic Restriction.

Answer: D

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/elb-capture-client-ip-addresses/

NEW QUESTION 35
Your company has a 1-Gbps AWS Direct Connect connection to AWS. Your company needs to send traffic from on-premises to a VPC owned by a partner company. The connectivity must have minimal latency at the lowest price.
Which of the following connectivity options should you choose?

A. Create a new Direct Connect connection, and set up a new circuit to connect to the partner VPC using a private virtual interface.
B. Create a new Direct Connect connection, and leverage the existing circuit to connect to the partner VPC.
C. Create a new private virtual interface, and leverage the existing connection to connect to the partner VPC.
D. Enable VPC peering and use your VPC as a transitive point to reach the partner VPC.

Answer: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/create-vpc-peering-connection.html#create-vpc-peering-connec

NEW QUESTION 36
A VPC is deployed with a 10 0 0.0/16 CIDR block. The engineering team is reviewing DHCP options and there is disagreement about the valid DNS addresses available for the VPC Which addresses are valid IP addresses provided by Amazon for this subnet' (Select TWO.)

A. 8.8.8.8
B. 10.00.2
C. 10.1.0.2
D. 169.254.169.253
E. 169.254.169.254

Answer: BE

NEW QUESTION 39
A company uses an AWS Site-to-Site VPN to connect its corporate network The company recently added an AWS Direct Connect connection A network engineer wants all traffic to use the Direct Connect connection and for the VPN to be used as backup However after the Direct Connect connection was added traffic continued to pass through the VPN connection
What should the network engineer do to route the traffic through the Direct Connect connection'?

A. Add routes to the VPC route tables that specify the Direct Connect connection
B. Set local preference BGP community tags on the on-premises router
C. Advertise the same network routes over the Direct Connect connection and VPN connection
D. Ensure the Direct Connect connection AS_PATH is longer than the VPN connection AS_PATH

Answer: C

NEW QUESTION 40
Your company has set up AWS Direct Connect to connect on-premises to an Amazon VPC instance. Two Direct Connect connections terminate at two different Direct Connect locations. You are using two routers, R1 and R2, at your end (one of each Direct Connect connection). R1 and R2 do NOT have connectivity between them. Both routers advertise the same routers over BGP to the VGW. You have a stateful firewall on each router. The routers drop some of the traffic coming from the VPC.
Which two actions should you take to fix this problem? (Select two.)

A. Use BGP AS prepend attribute to prepend additional AS numbers while advertising routers from R1 to VGW.
B. Use BGP local preference attribute to assign R1 to a lower local preference number than R2.
C. Use BGP local preference attribute to assign R1 a higher local preference number than R2.

D. Use BGP MED attribute to assign a higher MED value to the routes advertised R1 to VGW.
E. Use BGP MED attribute to assign a higher MED value to the routes advertised from R2 to VGW.

Answer: AD

NEW QUESTION 41
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.

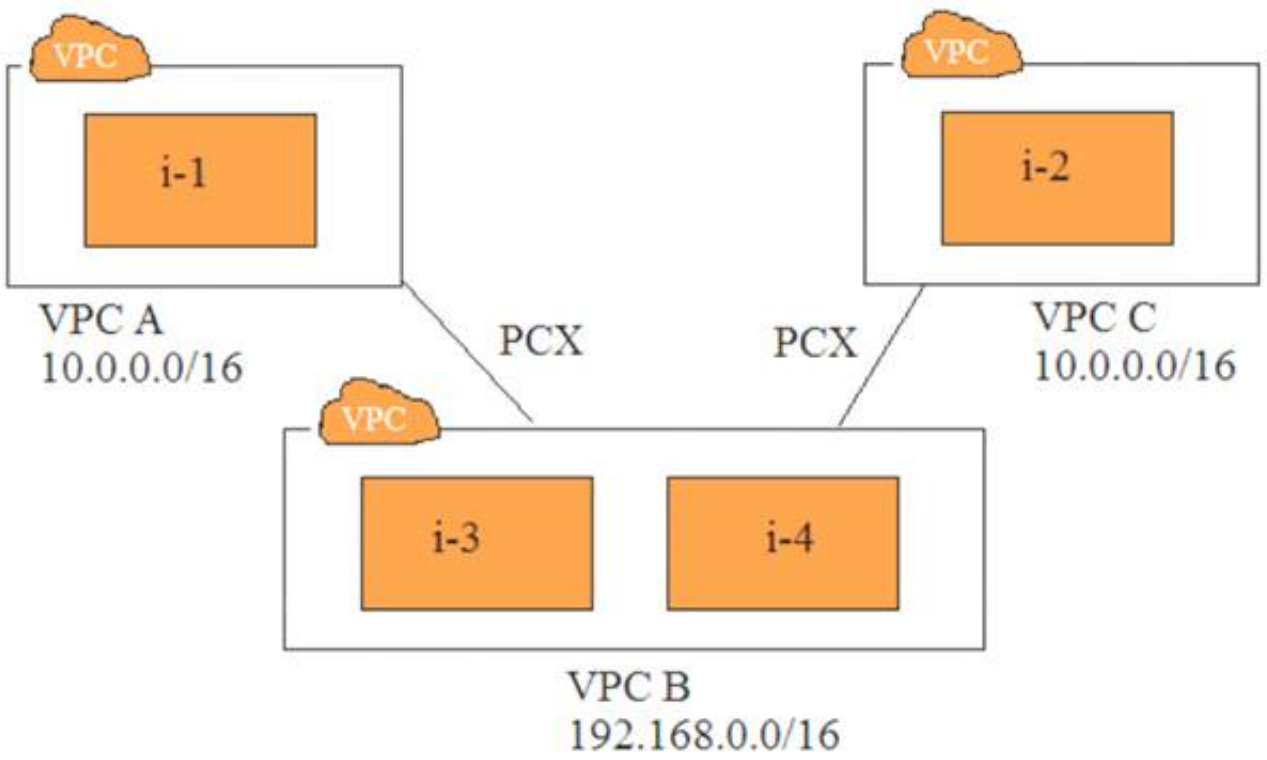
Answer: D

NEW QUESTION 44
A Network Engineer has enabled VPC Flow Logs to troubleshoot an ICMP reachability issue for an echo reply from an Amazon EC2 instance. The flow logs reveal an ACCEPT record for the request from the client to the EC2 instance, and a REJECT record for the response from the EC2 instance to the client.
What is the MOST likely reason for there to be a REJECT record?

A. The security group is denying inbound ICMP.
B. The network ACL is denying inbound ICMP.
C. The security group is denying outbound ICMP.
D. The network ACL is denying outbound ICMP.

Answer: D

NEW QUESTION 47
Refer to the image.



You have three VPCs: A, B, and C. VPCs A and C are both peered with VPC B. The IP address ranges are as follows:
VPC A: 10.0.0.0/16
VPC B: 192.168.0.0/16
VPC C: 10.0.0.0/16
Instance i-1 in VPC A has the IP address 10.0.0.10. Instance i-2 in VPC C has the IP address 10.0.0.10. Instances i-3 and i-4 in VPC B have the IP addresses 192.168.1.10 and 192.168.1.20, respectively, i-3 and i-4 are in the subnet 192.168.1.0/24.
i-3 must be able to communicate with i-1
i-4 must be able to communicate with i-2
i-3 and i-4 are able to communicate with i-1, but not with i-2.
Which two steps will fix this problem? (Select two.)

A. Create subnets 192.168.1.0/28 and 192.168.1.16/28. Move i-3 and i-4 to these subnets, respectively.
B. Create subnets 192.168.1.0/27 and 192.168.1.16/27. Move i-3 and i-4 to these subnets, respectively.
C. Change the IP address of i-2 to 10.0.0.100. Assign it an elastic IP address.
D. Create a new route table for VPC B, with unique route entries for destination VPC A and destination VPC C.
E. Create two route tables: one with a route for destination VPC A, and another for destination VPC C.

Answer: AE

Explanation:
https://docs.aws.amazon.com/vpc/latest/peering/peering-configurations-partial-access.html#one-to-two-vpcs-sim

NEW QUESTION 52
A Network Engineer is designing a new system on AWS that will take advantage of Amazon CloudFront for both content caching and for protecting the underlying origin. There is concern that an external agency might be able to access the IP addresses for the application's origin and then attack the origin despite it being served by CloudFront. Which of the following solutions provides the strongest level of protection to the origin?

A. Use an IP whitelist rule in AWS WAF within CloudFront to ensure that only known-client IPs are able to access the application.
B. Configure CloudFront to use a custom header and configure an AWS WAF rule on the origin's Application Load Balancer to accept only traffic that contains that header.
C. Configure an AWS Lambda@Edge function to validate that the traffic to the Application Load Balancer originates from CloudFront.
D. Attach an origin access identity to the CloudFront origin that allows traffic to the origin that originates from only CloudFront.

Answer: B

NEW QUESTION 55
A network engineer is managing two AWS Direct Connect connections. Each connection has a public virtual interface configured with a private ASN. The engineer wants to configure active/passive routing between the Direct Connect connections to access Amazon public endpoints. What BGP configuration is required for the on-premises equipment? (Select two.)

A. Use Local Pref to control outbound traffic.
B. Use AS Prepending to control inbound traffic.
C. Use eBGP multi-hop between loopback interfaces.
D. Use BGP Communities to control outbound traffic.
E. Advertise more specific prefixes over one Direct Connect connection.

Answer: AE

Explanation:
https://aws.amazon.com/premiumsupport/knowledge-center/active-passive-direct-connect/

NEW QUESTION 56
Your application is hosted behind an Elastic Load Balancer (ELB) within an autoscaling group. The autoscaling group is configured with a minimum of 2, a maximum of 14, and a desired value of 2. The autoscaling cooldown and the termination policies are set to the default value.
CloudWatch reports that the site typically requires just two servers, but spikes at the start and end of the business day can require eight to ten servers. You receive intermittent reports of timeouts and partially loaded web pages.
Which configuration change should you make to address this issue?

A. Configure connection draining on the ELB.
B. Configure the autoscaling cooldown to 600 seconds.
C. Configure the termination policy to oldest instance.
D. Configure a Terminating: Wait lifecycle hook on a scale in event.

Answer: A

Explanation:
References: https://docs.aws.amazon.com/autoscaling/ec2/userguide/attach-load-balancer-asg.html

NEW QUESTION 58
A space exploration company owns a series of telescopes that capture a large number of images and data of the night sky. The images and data are processed on an application hosted on AWS Fargate in a target group assigned to an Application Load Balancer (ALB). The application is made available through the address https:/'space example com
Scientists require another custom-built application hosted on several Amazon EC2 instances within an Auto Scaling group. This application will be made available from the address https://space.example.com/meteor. The company needs a solution that can automatically scale from a small number of requests overnight to a large number of requests for a future meteor shower.
What is the MOST operationally efficient solution that meets these requirements?

A. Update the existing target group with the new EC2 instance
B. Update the application's ALB by adding a listener rule that redirects /meteor to the newly added EC2 instances.
C. Create a new target grou
D. Configure the Auto Scaling group of the EC2 instances to use the target group Update the ALB by adding a listener rule that redirects /meteor to the new target group.
E. Create a Network Load Balancer (NLB). Configure the NLB to listen on two port
F. Configure a target group for one port to deliver all IP traffic to the Auto Scaling group to process the custom image
G. Configure a target group for the second port to deliver all IP traffic to Fargate Use path-based routing in the ALB to route traffic for the URL prefix /meteor to the first target grou
H. Route all other paths to the second target group.
I. Place the ALB behind an Amazon CloudFront distributio
J. Create a Lambda@Edge function that parses the request URI and adds the path-pattern header with the IP addresses of the EC2 instances to any request for /meteo
K. Add a listener rule to the ALB that looks for the HTTP header and uses the IP addresses of the EC2 instances to forward the traffic.

Answer: A

NEW QUESTION 59
An organization is deploying an application in a VPC that requires SSL mutual authentication with a client-side certificate, as that is the primary method of identifying clients. The Network Engineer has been tasked with defining the mechanism used within AWS to provide the SSL mutual authentication.

Which of the following options meets the organization's requirements?

A. Use a Classic Load Balancer and upload the client certificate private keys to i
B. Perform SSL mutual authentication of the client-side certificate there.
C. Use a Network Load Balancer with a TCP listener on port 443, and pass the request through for the SSL mutual authentication to be handled by a backend instance.
D. Use an Application Load Balancer and upload the client certificate private keys to it by using the native server name indication (SNI) features with smart certificate selection to handle multiple calling applications.
E. Front the application with Amazon API Gateway, and use its client-side SSL mutual authentication feature that uses the backend instances to verify the source of the request.

Answer: B

NEW QUESTION 62
A network architect is designing an internet website. It has web, application, and database tiers that will run in AWS. The website uses Amazon DynamoDB.
Which architecture will minimize public exposure of the back-end instances?

A. A VPC with public subnets for the NLB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
B. A VPC with public subnets for the ALB, private subnets for the web tier, and private subnets for the application tie
C. The application tier connects DynamoDB through a VPC endpoint.
D. A VPC with public subnets for the ALB, public subnets for the web tier, private subnets for the application tier, and private subnets for DynamoDB.
E. A VPC with public subnets for the NLB, private subnets for the web tier, and public subnets for theapplication tie
F. The application tier connects DynamoDB through a VPC endpoint.

Answer: B

NEW QUESTION 67
A company is about to migrate an application from its on-premises data center to AWS. As part of the planning process, the following requirements involving DNS have been identified.
The organization’s VPC uses the CIDR block 172.16.0.0/16.
Assuming that there is no DNS namespace overlap, how can these requirements be met?

A. Change the DHCP options set for the VPC to use both the Amazon-provided DNS server and theon-premises DNS system
B. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
C. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxie
D. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to 172.16.0.2. Change the DHCP options set for the VPC to use the new DNS proxie
E. Configure the on-premises DNS systems with a stub-zone, delegating the name server 172.16.0.2 as authoritative for the Route 53 private hosted zone.
F. Deploy and configure a set of EC2 instances into the company VPC to act as DNS proxie
G. Configure the proxies to forward queries for the on-premises domain to the on-premises DNS systems, and forward all other queries to the Amazon-provided DNS server (172.16.0.2). Change the DHCP options set for the VPC to use the new DNS proxie
H. Configure the on-premises DNS systems with a stub-zone, delegating the proxies as authoritative for the Route 53 private hosted zone.
I. Change the DHCP options set for the VPC to use both the on-premises DNS system
J. Configure theon-premises DNS systems with a stub-zone, delegating the Route 53 private hosted zone’s name servers as authoritative for the Route 53 private hosted zone.

Answer: C

NEW QUESTION 71
A customer is using ABC Telecom as a network provider. The customer has 10 different offices connected to ABC Telecom’s MPLS backbone. The customer is setting up an AWS Direct Connect connection to AWS and has provided the LOA-CFA to ABC Telecom. ABC Telecom has terminated the Direct Connect circuit into their MPLS backbone. To uniquely identify the customer’s traffic over the MPLS backbone, the customer must encapsulate all traffic with VLAN tag 100. The customer wants to send traffic to multiple VPCs.
Which two steps should be taken to meet the customer’s requirement? (Select two.)

A. The customer performs Q-in-Q tunneling, with the AWS-required VLAN tag in the inside and VLAN 100 as the outside tag.
B. Create a support ticket with AWS to request the removal of the outer VLAN tag 100 as the traffic reaches AWS routers.
C. Send the traffic for all VPCs with the same VLAN tag 100 and use BGP to ensure that proper routing takes place to the appropriate VPC.
D. ABC Telecom removes the other tag before sending the packet to AWS.
E. ABC Telecom creates a support ticket with AWS to exchange MPLS labels and include the AWS port as part of their MPLS network.

Answer: AD

NEW QUESTION 75
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your AWS-Certified-Advanced-Networking-Specialty Exam with Our Prep Materials Via below:

https://www.certleader.com/AWS-Certified-Advanced-Networking-Specialty-dumps.html