ANS-C01$^{\text{Q\&As}}$

AWS Certified Advanced Networking Specialty Exam

QUESTION 1

A retail company is running its service on AWS. The company\\'s architecture includes Application Load Balancers (ALBs) in public subnets. TheALB target groups are configured to send traffic to backend Amazon EC2 instances in private subnets. These backend EC2 instances can callexternally 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 ofthis 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 interface. Publish the logs to a log group in Amazon CloudWatch Logs. UseCloudWatch Logs Insights to query and analyze the logs.

B. Enable NAT gateway access logs. Publish the logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to queryand analyze the logs.

C. Configure Traffic Mirroring on the NAT gateway\\'s elastic network interface. Send the traffic to an additional EC2 instance. Use tools suchas tcpdump and Wireshark to query and analyze the mirrored traffic.

D. Enable VPC flow logs on the NAT gateway\\'s elastic network interface. Publish the logs to an Amazon S3 bucket. Create a custom tablefor the S3 bucket in Amazon Athena to describe the log structure. Use Athena to query and analyze the logs.

E. Enable NAT gateway access logs. Publish the logs to an Amazon S3 bucket. Create a custom table for the S3 bucket in Amazon Athenato describe the log structure. Use Athena to query and analyze the logs.

Correct Answer: AD

A. Yes, this would work.

B. Not a real thing, wrong

C. We don\\'t need to do packet inspection to analyze costs. This won\\'t help with costs at all.

D. The most obvious right answer.

E. Like B, not a real thing.

QUESTION 2

An IoT company sells hardware sensor modules that periodically send out temperature, humidity, pressure, and location data through theMQTT messaging protocol. The hardware sensor modules send this data to the company\\'s on-premises MQTT brokers that run on Linux serversbehind 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 additionallatency because of the company\\'s global presence. As a result, the company decides to migrate its entire infrastructure from on premises tothe AWS Cloud. The company needs to migrate without reconfiguring the hardware sensor modules that are already deployed across theworld. 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 listeners. Use Bring Your Own IP (BYOIP) from the on-premises network with the NLB.

B. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listeners. Create an AWS Global

Accelerator acceleratorin front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator.

C. Place the EC2 instances behind an Application Load Balancer (ALB). Configure TCP listeners. Create an AWS Global Acceleratoraccelerator in front of the ALB. Use Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator

D. Place the EC2 instances behind an Amazon CloudFront distribution. Use Bring Your Own IP (BYOIP) from the on-premises network withCloudFront.

Correct Answer: B

https://aws.amazon.com/blogs/iot/creating-static-ip-addresses-and-custom-domains-for-aws-iot-core-endpoints/

QUESTION 3

A company has deployed an AWS Network Firewall firewall into a VPC. A network engineer needs to implement a solution to deliver NetworkFirewall 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 bucket. Create an AWS Lambda function to load logs into the Amazon OpenSearch Service (Amazon ElasticsearchService) cluster. Enable Amazon Simple Notification Service (Amazon SNS) notifications on the S3 bucket to invoke the Lambda function.Configure flow logs for the firewall. Set the S3 bucket as the destination.

B. Create an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service)cluster as the destination. Configure flow logs for the firewall Set the Kinesis Data Firehose delivery stream as the destination for theNetwork Firewall flow logs.

C. Configure flow logs for the firewall. Set the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination forthe Network Firewall flow logs.

D. Create an Amazon Kinesis data stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as thedestination. Configure flow logs for the firewall. Set the Kinesis data stream as the destination for the Network Firewall flow logs.

Correct Answer: B

https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-analyze-aws-network-firewall-logs-using-amazon-opensearch-service-part-1/

QUESTION 4

A network engineer needs to deploy an AWS Network Firewall firewall into an existing AWS environment. The environment consists of thefollowing:. A transit gateway with all VPCs attached to it. Several hundred application VPCs. A centralized egress internet VPC with a NAT gateway and an internet gateway. A centralized ingress internet VPC that hosts public Application Load Balancers. On-premises connectivity through an AWS Direct Connect gateway attachmentThe application VPCs have workloads deployed across multiple Availability Zones in private subnets with the VPC route table s default route(0.0.0.0/0) pointing to the transit gateway. The Network Firewall firewall needs to inspect east-west (VPC-to-VPC) traffic and north-south(internet-bound and on-premises network) traffic by using Suricata compatible rules.The network engineer must deploy the firewall by using a solution that requires the least possible architectural changes to the existingproduction environment.Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Deploy Network Firewall in all Availability Zones in each application VPC.

B. Deploy Network Firewall in all Availability Zones in a centralized inspection VPC.

C. Update the HOME_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks.

D. Update the EXTERNAL_NET rule group variable to include all CIDR ranges of the VPCs and on-premises networks.

E. Configure a single transit gateway route table. Associate all application VPCs and the centralized inspection VPC with this route table.

F. Configure two transit gateway route tables. Associate all application VPCs with one transit gateway route table. Associate thecentralized inspection VPC with the other transit gateway route table.

Correct Answer: BCF

Option B: A centralized inspection VPC approach would lead to a minimal architectural change and efficiently use Network Firewall resources. Option C: HOME_NET is usually defined as your local network. In this case, it would include all your VPCs and on-premises networks.

Option F: Configuring two transit gateway route tables, one associated with all the application VPCs and another with the inspection VPC, will help route traffic effectively for inspection. All outbound traffic from application VPCs would be routed to the inspection VPC for firewall checks, and then the inspected traffic would be routed to its destination (internet or another VPC).

QUESTION 5

A company has two AWS accounts one for Production and one for Connectivity. A network engineer needs to connect the Production accountVPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.Which set of steps should the network engineer follow in each AWS account to meet these requirements?

A. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide theConnectivity account ID. Enable the feature to allow external accounts2. In the Connectivity account: Accept the resource.3. In the Connectivity account: Create an attachment to the VPC subnets.4. In the Production account: Accept the attachment. Associate a route table with the attachment.

B. 1. In the Production account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Connectivityaccount ID. Enable the feature to allow external accounts.2. In the Connectivity account: Accept the resource.3. In the Production account: Create an attachment on the transit gateway to the VPC subnets.4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment.

C. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the VPC subnets. Provide the Productionaccount ID. Enable the feature to allow external accounts.2. In the Production account: Accept the resource.3. In the Connectivity account: Create an attachment on the transit gateway to the VPC subnets.4. In the Production account: Accept the attachment. Associate a route table with the attachment.

D. 1. In the Connectivity account: Create a resource share in AWS Resource Access Manager for the transit gateway. Provide theProduction account ID Enable the feature to allow external accounts.2. In the Production account: Accept the resource.3. In the Production account: Create an attachment to the VPC subnets.4. In the Connectivity account: Accept the attachment. Associate a route table with the attachment.

Correct Answer: D

D is correct, the first step is to share the TGW From the Connectivity account to the Production account, making all the other options incorrect.