ANS-C01 Q&As

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

QUESTION 1

A company is running multiple workloads on Amazon EC2 instances in public subnets. In a recent incident, an attacker exploited anapplication vulnerability on one of the EC2 instances to gain access to the instance. The company fixed the application and launched areplacement EC2 instance that contains the updated application.The attacker used the compromised application to spread malware over the internet. The company became aware of the compromise througha notification from AWS. The company needs the ability to identify when an application that is deployed on an EC2 instance is spreadingmalware.Which solution will meet this requirement with the LEAST operational effort?

A. Use Amazon GuardDuty to analyze traffic patterns by inspecting DNS requests and VPC flow logs.

B. Use Amazon GuardDuty to deploy AWS managed decoy systems that are equipped with the most recent malware signatures.

C. Set up a Gateway Load Balancer. Run an intrusion detection system (IDS) appliance from AWS Marketplace on Amazon EC2 for trafficinspection.

D. Configure Amazon Inspector to perform deep packet inspection of outgoing traffic.

Correct Answer: A

This solution involves using Amazon GuardDuty to monitor network traffic and analyze DNS requests and VPC flow logs for suspicious activity. This will allow the company to identify when an application is spreading malware by monitoring the network traffic patterns associated with the instance. GuardDuty is a fully managed threat detection service that continuously monitors for malicious activity and unauthorized behavior in your AWS accounts and workloads. It requires minimal setup and configuration and can be integrated with other AWS services for automated remediation. This solution requires the least operational effort compared to the other options

QUESTION 2

A company\\'s existing AWS environment contains public application servers that run on Amazon EC2 instances. The application servers run in aVPC subnet. Each server is associated with an Elastic IP address.The company has a new requirement for firewall inspection of all traffic from the internet before the traffic reaches any EC2 instances. Asecurity engineer has deployed and configured a Gateway Load Balancer (GLB) in a standalone VPC with a fleet of third-party firewalls.How should a network engineer update the environment to ensure that the traffic travels across the fleet of firewalls?

A. Deploy a transit gateway. Attach a GLB endpoint to the transit gateway. Attach the application VPC to the transit gateway. Update theapplication subnet route table\\'s default route destination to be the GLB endpoint. Ensure that the EC2 instances\\' security group allowstraffic from the GLB endpoint.

B. Update the application subnet route table to have a default route to the GLOn the standalone VPC that contains the firewall fleet, add aroute in the route table for the application VPC\\'s CIDR block with the GLB endpoint as the destination. Update the EC2 instances\\' securitygroup to allow traffic from the GLB.

C. Provision a GLB endpoint in the application VPC in a new subnet. Create a gateway route table with a route that specifies theapplication subnet CIDR block as the destination and the GLB endpoint as the target. Associate the gateway route table with the internetgateway in the application VPUpdate the application subnet route table\\'s default route destination to be the GLB endpoint.

D. Instruct the security engineer to move the GLB into the application VPC. Create a gateway route table. Associate the gateway routetable with the application subnet. Add a default route to the gateway route table with the GLB as its destination. Update the route tableon the GLB to direct traffic from the internet gateway to the application servers.

Ensure that the EC2 instances\\' security group allowstraffic from the GLB.

Correct Answer: C

A is incorrect -> attach a GWLB endpoint to transit gateway???

B is incorrect - need to inspect all traffic FROM the Internet, not the other way

D. is incorrect -> IGW needs a route to re-direct traffic to GWLB, you can\\'t do that from GWLB\\'s route table.

QUESTION 3

A network engineer has deployed an Amazon EC2 instance in a private subnet in a VPC. The VPC has no public subnet. The EC2 instancehosts application code that sends messages to an Amazon Simple Queue Service (Amazon SQS) queue. The subnet has the default networkACL 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

Correct Answer: AC

A - EC2 requires IAM role that allows write operations to Amazon SQS C - Being in private subnet, interface endpoint is required to access SQS

QUESTION 4

A company has expanded its network to the AWS Cloud by using a hybrid architecture with multiple AWS accounts. The company has set up ashared AWS account for the connection to its on-premises data centers and the company offices. The workloads consist of private web-basedservices for internal use. These services run in different AWS accounts. Office-based employees consume these services by using a DNS namein 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 processinvolves many teams.The company wants to update the DNS registration process by giving the service creators access that will allow them to register their DNSrecords. A network engineer must design a solution that will achieve this goal. The solution must maximize cost-effectiveness and mustrequire 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 tothe employees who need access.

B. Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain namedaws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint\\'s IP addresses that werecreated.

C. Create an Amazon Route 53 Resolver rule to forward any queries made to onprem.example.internal to the on-premises DNS servers.

D. Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for thisdomain.

E. Launch two Amazon EC2 instances in the shared AWS account. Install BIND on each instance. Create a DNS conditional forwarder oneach BIND server to forward queries for each subdomain under aws.example.internal to the appropriate private hosted zone in each AWSaccount. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IPaddresses to the IP addresses of the BIND servers.

F. Create a private hosted zone in the shared AWS account for each account that runs the service. Configure the private hosted zone tocontain aws.example.internal in the domain (account1.aws.example.internal). Associate the private hosted zone with the VPC that runsthe service and the shared account VPC.

Correct Answer: BDF

Inbound resolver endpoint and forwarder rule in on-premises DNS Servers, Private Hosted Zones for aws.example.internal and sub domain delegation to respective services (service.aws.example.internal), and association the sub domain private hosted zones with respective VPCs in other accounts.

QUESTION 5

A company\\'s network engineer needs to design a new solution to help troubleshoot and detect network anomalies. The network engineer hasconfigured Traffic Mirroring. However, the mirrored traffic is overwhelming the Amazon EC2 instance that is the traffic mirror target. The EC2instance hosts tools that the company\\'s security team uses to analyze the traffic. The network engineer needs to design a highly availablesolution 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 target. Behind the NLB. deploy a fleet of EC2 instances in an Auto Scalinggroup. Use Traffic Mirroring as necessary.

B. Deploy an Application Load Balancer (ALB) as the traffic mirror target. Behind the ALB, deploy a fleet of EC2 instances in an AutoScaling group. Use Traffic Mirroring only during non-business hours.

C. Deploy a Gateway Load Balancer (GLB) as the traffic mirror target. Behind the GLB. deploy a fleet of EC2 instances in an Auto Scalinggroup. Use Traffic Mirroring as necessary.

D. Deploy an Application Load Balancer (ALB) with an HTTPS listener as the traffic mirror target. Behind the ALB. deploy a fleet of EC2instances in an Auto Scaling group. Use Traffic Mirroring only during active events or business hours.

Correct Answer: A

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-targets.html

ANS-C01 Practice Test   ANS-C01 Study Guide   ANS-C01 Exam Questions