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

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/ans-c01.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- Instant Download After Purchase
- 100% Money Back Guarantee
- 365 Days Free Update
- 800,000+ Satisfied Customers

SATISFACTION GUARANTEED
100%
SATISFACTION GUARANTEED

QUESTION 1

A company has deployed an application in a VPC that uses a NAT gateway for outbound traffic to the internet. A network engineer notices alarge quantity of suspicious network traffic that is traveling from the VPC over the internet to IP addresses that are included on a deny list.The network engineer must implement a solution to determine which AWS resources are generating the suspicious traffic. The solution mustminimize cost and administrative overhead.Which solution will meet these requirements?

A. Launch an Amazon EC2 instance in the VPC. Use Traffic Mirroring by specifying the NAT gateway as the source and the EC2 instance asthe destination. Analyze the captured traffic by using open-source tools to identify the AWS resources that are generating the suspicioustraffic.

B. Use VPC flow logs. Launch a security information and event management (SIEM) solution in the VPC. Configure the SIEM solution toingest the VPC flow logs. Run queries on the SIEM solution to identify the AWS resources that are generating the suspicious traffic.

C. Use VPC flow logs. Publish the flow logs to a log group in Amazon CloudWatch Logs. Use CloudWatch Logs Insights to query the flowlogs to identify the AWS resources that are generating the suspicious traffic.

D. Configure the VPC to stream the network traffic directly to an Amazon Kinesis data stream. Send the data from the Kinesis data streamto an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Athena to query the data to identify theAWS resources that are generating the suspicious traffic.

Correct Answer: C

The solution must minimize cost and administrative overhead

QUESTION 2

A company\\'s application team is unable to launch new resources into its VPC. A network engineer discovers that the VPC has run out ofusable IP addresses. The VPC CIDR block is 172.16.0.0/16.Which additional CIDR block can the network engineer attach to the VPC?

A. 172.17.0.0/29

B. 10.0.0.0/16

C. 172.17.0.0/16

D. 192.168.0.0/16

Correct Answer: C

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-cidr-blocks.html#add-cidr-block-restrictions Only it will also us to add 172.17.0.0/16

QUESTION 3

A network engineer must provide additional safeguards to protect encrypted data at Application Load Balancers (ALBs) through the use of aunique random session key.What should the network engineer do to meet this requirement?

A. Change the ALB security policy to a policy that supports TLS 1.2 protocol only

B. Use AWS Key Management Service (AWS KMS) to encrypt session keys

C. Associate an AWS WAF web ACL with the ALBs. and create a security rule to enforce forward secrecy (FS)

D. Change the ALB security policy to a policy that supports forward secrecy (FS)

Correct Answer: D

Use ELBSecurityPolicy-FS policies, if you require Forward Secrecy Provides additional safeguards against the eavesdropping of encrypted data Using a unique random session key

QUESTION 4

A company is establishing connectivity between its on-premises site and an existing VPC on AWS to meet a new security requirement.According to the new requirement, all public DNS queries must use an on-premises DNS security solution. The company\\'s security team hasallowed an exception for the AWS service endpoints because the company is using VPC endpoints to access AWS services.Which combination of steps should a network engineer take to configure the architecture to meet these requirements? (Choose three.)

A. Create a system rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

B. Create a new DHCP options set that provides the IP address of the on-premises DNS security solution. Update the VPC to use this newDHCP options set.

C. Create an Amazon Route 53 Resolver inbound endpoint. Associate this endpoint with the VPC.

D. Create an Amazon Route 53 Resolver outbound endpoint. Associate this endpoint with the VPC.

E. Create a system rule for the domain name amazonaws.com.

F. Create a forwarding rule for the domain name "." (dot) with a target IP address of the on-premises DNS security solution.

Correct Answer: DEF

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-overview-DSN-queries-to-vpc.html#resolver-overview-forward-vpc-to-network-autodefined-rules

QUESTION 5

A company hosts a web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instancesare in an Auto Scaling group. The company uses an Amazon CloudFront distribution with the ALB as an origin.The application recently experienced an attack. In response, the company associated an AWS WAF web ACL with the CloudFront distribution.The company needs to use Amazon Athena to analyze application attacks that AWS WAF detects.Which solution will meet this requirement?

A. Configure the ALB and the EC2 instance subnets to produce VPC flow logs. Configure the VPC flow logs to deliver logs to an Amazon S3bucket for log analysis.

B. Create a trail in AWS CloudTrail to capture data events. Configure the trail to deliver logs to an Amazon S3 bucket for log analysis.

C. Configure the AWS WAF web ACL to deliver logs to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliverthe data to an Amazon S3 bucket for log analysis.

D. Turn on access logging for the ALB. Configure the access logs to deliver the logs to an Amazon S3 bucket for log analysis.

Correct Answer: C

To send logs to Amazon Kinesis Data Firehose, you send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, AWS WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose.

Latest ANS-C01 Dumps   ANS-C01 PDF Dumps   ANS-C01 Practice Test