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

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

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

QUESTION 1

A security team is performing an audit of a company\\'s AWS deployment. The security team is concerned that two applications might beaccessing resources that should be blocked by network ACLs and security groups. The applications are deployed across two Amazon ElasticKubernetes Service (Amazon EKS) clusters that use the Amazon VPC Container Network Interface (CNI) plugin for Kubernetes. The clustersare in separate subnets within the same VPC and have a Cluster Autoscaler configured.The security team needs to determine which POD IP addresses are communicating with which services throughout the VPC. The security teamwants to limit the number of flow logs and wants to examine the traffic from only the two applications.Which solution will meet these requirements with the LEAST operational overhead?

A. Create VPC flow logs in the default format. Create a filter to gather flow logs only from the EKS nodes. Include the srcaddr field and thedstaddr field in the flow logs.

B. Create VPC flow logs in a custom format. Set the EKS nodes as the resource Include the pkt-srcaddr field and the pkt-dstaddr field in theflow logs.

C. Create VPC flow logs in a custom format. Set the application subnets as resources. Include the pkt-srcaddr field and the pkt-dstaddrfield in the flow logs.

D. Create VPC flow logs in a custom format. Create a filter to gather flow logs only from the EKS nodes. Include the pkt-srcaddr field andthe pkt-dstaddr field in the flow logs.

Correct Answer: C

Eks Node can\\'t be specified in VPC log filter

QUESTION 2

AnyCompany has acquired Example Corp. AnyCompany\\'s infrastructure is all on premises, and Example Corp\\'s infrastructure is completely inthe AWS Cloud. The companies are using AWS Direct Connect with AWS Transit Gateway to establish connectivity between each other.Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway. The CIDR range for the VPC is10.0.0.0/16. Example Corp needs to access an application that is deployed on premises by AnyCompany. Because of compliancerequirements, Example Corp must access the application through a limited contiguous block of approved IP addresses (10.1.0.0/24).A network engineer needs to implement a highly available solution to achieve this goal. The network engineer starts by updating the VPC toadd a new CIDR range of 10.1.0.0/24.What should the network engineer do next to meet the requirements?

A. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a public NAT gateway ineach of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the public NATgateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the public NATgateways to send traffic destined for the application to the transit gateway.

B. In each Availability Zone in the VPC, create a subnet that uses part of the allowed IP address range. Create a private NAT gateway ineach of the new subnets. Update the route tables that are associated with other subnets to route application traffic to the private NATgateway in the corresponding Availability Zone. Add a route to the route table that is associated with the subnets of the private NATgateways to send traffic destined for the application to the transit gateway.

C. In the VPC, create a subnet that uses the allowed IP address range. Create a private NAT gateway in the new subnet. Update the routetables that are associated with other subnets to route application traffic to the private NAT gateway.

Add a route to the route table that isassociated with the subnet of the private NAT gateway to send traffic destined for the application to the transit gateway.

D. In the VPC, create a subnet that uses the allowed IP address range. Create a public NAT gateway in the new subnet. Update the routetables that are associated with other subnets to route application traffic to the public NAT gateway. Add a route to the route table that isassociated with the subnet of the public NAT gateway to send traffic destined for the application to the transit gateway.

Correct Answer: B

B is correct - Needs to be highly available so multiple AZ\\'s required one in each of the 2 AZ\\'s

"Example Corp has deployed a new application across two Availability Zones in a VPC with no internet gateway"

QUESTION 3

A company delivers applications over the internet. An Amazon Route 53 public hosted zone is the authoritative DNS service for the companyand its internet applications, all of which are offered from the same domain name.A network engineer is working on a new version of one of the applications. All the application\\'s components are hosted in the AWS Cloud. Theapplication has a three-tier design. The front end is delivered through Amazon EC2 instances that are deployed in public subnets with ElasticIP addresses assigned. The backend components are deployed in private subnets from RFC1918.Components of the application need to be able to access other components of the application within the application\\'s VPC by using the samehost names as the host names that are used over the public internet. The network engineer also needs to accommodate future DNS changes,such as the introduction of new host names or the retirement of DNS entries.Which combination of steps will meet these requirements? (Choose three.)

A. Add a geoproximity routing policy in Route 53.

B. Create a Route 53 private hosted zone for the same domain name Associate the application\\'s VPC with the new private hosted zone.

C. Enable DNS hostnames for the application\\'s VPC.

D. Create entries in the private hosted zone for each name in the public hosted zone by using the corresponding private IP addresses.

E. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that runs when AWS CloudTrail logs a Route 53 API call to the publichosted zone. Create an AWS Lambda function as the target of the rule. Configure the function to use the event information to update theprivate hosted zone.

F. Add the private IP addresses in the existing Route 53 public hosted zone.

Correct Answer: BCD

B - you need a priavte hosted zone to resolve the same names to private IPs C - this one is tricky but you really need both of the DNS options enbaled in the VPC (enableDnsHostnames and enableDnsSupport) https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-hostnames "If you use custom DNS domain names defined in a private hosted zone in Amazon Route 53, or use private DNS with interface VPC endpoints (AWS PrivateLink), you must set both the enableDnsHostnames and enableDnsSupport attributes to true." D - This is correct A - wrong - no need to explain E - Nobody is asking to autmoate the process F - This will simply not work as you need records to resolve to both private nad poublic, yu must have two zones

QUESTION 4

A company\\'s network engineer must implement a cloud-based networking environment for a network operations team to centrally manage. Other Teams will use the environment. Each team must be able to deploy infrastructure to the environment and must be able to manage its own resources. The environment must feature IPv4 and IPv6 support and must provide internet connectivity in a dual-stack configuration.

The company has an organization in AWS Organizations that contains a workload account for the teams. The network engineer creates a new networking account in the organization.

Which combination of steps should the network engineer take next to meet the requirements? (Choose three.)

A. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and specify an IPv6 block of 2001:db8:c5a:6000::/56. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPv6 CIDR blocks.

B. Create a new VPC. Associate an IPv4 CIDR block of 10.0.0.0/16 and use an Amazon-provided IPV6 CIDR block. Provision subnets by assigning /24 IPv4 CIDR blocks and /64 IPV6 CIDR blocks.

C. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the provisioned subnets, and share the provisioned subnets with the target workload account. Use the workload account to accept the resource share through AWS RAM.

D. Enable sharing of resources within the organization by using AWS Resource Access Manager (AWS RAM). Create a resource share in the networking account, select the new VPC, and share the new VPC with the target workload account. Use the workload account to accept the resource share through AWS RAM.

E. Create an internet gateway and an egress-only internal gateway. Deploy NAT gateways to the public subnets. Associate the internet gateway with the new VPC. Update the route tables. Associate the route tables with the relevant subnets.

F. Create an internet gateway. Deploy NAT instances to public subnets. Update the route tables. Associate the route tables with the relevant subnets.

Correct Answer: ACE

QUESTION 5

A company has an AWS environment that includes multiple VPCs that are connected by a transit gateway. The company has decided to useAWS Site-to-Site VPN to establish connectivity between its on-premises network and its AWS environment.The company does not have a static public IP address for its on-premises network. A network engineer must implement a solution to initiatethe VPN connection on the AWS side of the connection for traffic from the AWS environment to the on-premises network.Which combination of steps should the network engineer take to establish VPN connectivity between the transit gateway and the on-premisesnetwork? (Choose three.)

A. Configure the Site-to-Site VPN tunnel options to use Internet Key Exchange version 1 (IKEv1).

B. Configure the Site-to-Site VPN tunnel options to use Internet Key Exchange version 2 (IKEv2).

C. Use a private certificate authority (CA) from AWS Private Certificate Authority to create a certificate.

D. Use a public certificate authority (CA) from AWS Private Certificate Authority to create a certificate.

E. Create a customer gateway. Specify the current dynamic IP address of the customer gateway device\\'s external interface.

F. Create a customer gateway without specifying the IP address of the customer gateway device.

Correct Answer: BCF

https://docs.aws.amazon.com/vpn/latest/s2svpn/cgw-options.html#:~:text=(Optional)%20The%20IP,for%20more%20info.