Amazon

Exam Questions AWS-Certified-Advanced-Networking-Specialty

Amazon AWS Certified Advanced Networking - Specialty

NEW QUESTION 1
A company has two AWS accounts: one for Production and one for Connectivity. A network engineer needs to connect the Production account VPC to a transit gateway in the Connectivity account. The feature to auto accept shared attachments is not enabled on the transit gateway.
Which sot of stops should the network engineer follow in each AWS account to meet those requirements?

A. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the transit gateway Provide the Connectivity account ID Enable thefeature to allow external accounts* 2. 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 attachmen
B. Associate a route table with the attachment.
C. * 1. In the Production account Create a resource share In AWS Resource Access Manager for the VPC subnets Provide the Connectivity account 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 will the attachment.
D. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the VPC subnet
E. Provide the Production account ID Enable the feature lo 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 A In the Production account Accept the attachment Associate a route table with the attachment.
F. * 1. In the Connectivity account Create a resource share in AWS Resource Access Manager for the transit gateway Provide the Production 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 attachmen
G. Associate a route tab e win toe attachment

Answer: A

NEW QUESTION 2
Your company runs an application for the US market in the us-east-1 AWS region. This application uses proprietary TCP and UDP protocols on Amazon Elastic Compute Cloud (EC2) instances. End users run a
real-time, front-end application on their local PCs. This front-end application knows the DNS hostname of the service.
You must prepare the system for global expansion. The end users must access the application with lowest latency.
How should you use AWS services to meet these requirements?

A. Register the IP addresses of the service hosts as “A” records with latency-based routing policy in Amazon Route 53, and set a Route 53 health check for these hosts.
B. Set the Elastic Load Balancing (ELB) load balancer in front of the hosts of the service, and register the ELB name of the main service host as an ALIAS record with a latency-based routing policy in Route 53.
C. Set Amazon CloudFront in front of the host of the service, and register the CloudFront name of the main service as an ALIAS record in Route 53.
D. Set the Amazon API gateway in front of the service, and register the API gateway name of the main service as an ALIAS record in Route 53.

Answer: B

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
You are preparing to launch Amazon WorkSpaces and need to configure the appropriate networking resources. What must be configured to meet this requirement?

A. At least two subnets in different Availability Zones.
B. A dedicated VPC with Active Directory Services.
C. An IPsec VPN to on-premises Active Directory
D. Network address translation for outbound traffic.

Answer: AD

Explanation:
References: https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-vpc.html

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
An organization will be extending its existing on-premises infrastructure into the cloud. The design consists of a transit VPC that contains stateful firewalls that will be deployed in a highly available configuration across two Availability Zones for automatic failover.
What MUST be configured for this design to work? (Select two.)

A. A different Autonomous System Number (ASN) for each firewall.
B. Border Gateway Protocol (BGP) routing
C. Autonomous system (AS) path prepending
D. Static routing
E. Equal-cost multi-path routing (ECMP)

Answer: BC

Explanation:
https://docs.aws.amazon.com/solutions/latest/cisco-based-transit-vpc/appendix-a.html

NEW QUESTION 7
The Security department has mandated that all outbound traffic from a VPC toward an on-premises datacenter must go through a security appliance that runs on an Amazon EC2 instance.
Which of the following maximizes network performance on AWS? (Choose two.)

A. Support for the enhanced networking drivers
B. Support for sending traffic over the Direct Connect connection
C. The instance sizes and families supported by the security appliance
D. Support for placement groups within the VPC
E. Security appliance support for multiple elastic network interfaces

Answer: AC

NEW QUESTION 8
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 9
A company is connecting to a VPC over an AWS Direct Connect using a private VIF, and a dynamic VPN connection as a backup. The company's Reliability Engineering team has been running failover and resiliency tests on the network and the existing VPC by simulating an outage situation on the Direct Connect connection. During the resiliency tests, traffic failed to switch over to the backup VPN connection.
How can this failure be troubleshot?

A. Ensure that Bidirectional Forwarding Detection is enabled on the Direct Connect connection
B. Confirm that the same routes are being advertised over both the VPN and Direct Connect.
C. Reconfigure the Direct Connect session from static routes to Border Gateway Protocol (BGP) peering.
D. Configure a virtual private gateway for the VPN and another virtual private gateway for Direct Connect.

Answer: B

NEW QUESTION 10
A company has an application running on Amazon EC2 instances in a private subnet that connects to a
third-party service provider's public HTTP endpoint through a NAT gateway. As request rates increase, new connections are starting to fail. At the same time, the ErrorPortAllocation Amazon CloudWatch metric count for the NAT gateway is increasing.
Which of the following actions should improve the connectivity issues? (Choose two.)

A. Allocate additional elastic IP addresses to the NAT gateway.
B. Request that the third-party service provider implement HTTP keepalive.
C. Implement TCP keepalive on the client instances.
D. Create additional NAT gateways and update the private subnet route table to introduce the new NAT gateways.
E. Create additional NAT gateways in the public subnet and split client instances into multiple privatesubnets, each with a route to a different NAT gateway.

Answer: CE

NEW QUESTION 10
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 12
A company has recently established an AWS Direct Connect connection from its on-premises data center to AWS. A Network Engineer has blocked all traffic destined for Amazon S3 over the company's gateway to the internet from its on-premises firewall. S3 traffic should only traverse the Direct Connect connection. Currently, no one in the on-premises data center can access Amazon S3.
Which solution will resolve this connectivity issue?

A. Configure a private virtual interface on the Direct Connect connectio
B. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon S3.
C. Establish an S3 VPC endpoint for the company's Amazon VP
D. Configure a private virtual interface on the Direct Connect connectio
E. Update the on-premises routing tables to choose Direct Connect as the preferred next hop
F. Configure a public virtual interface on the Direct Connect connectio
G. Update the on-premises routing tables to choose Direct Connect as the preferred next hop for traffic destined for Amazon S3.
H. Configure a public virtual interface on the Direct Connect connectio
I. Establish an AWS managed VPN over the connectio
J. Update the on-premises routing tables to choose the VPN connection as the preferred next hop.

Answer: C

NEW QUESTION 16
A company has two redundant AWS Direct Connect connections to a VPC. The VPC is configured using BGP metrics so that one Direct Connect connection is used as the primary traffic path. The company wants the primary Direct Connect connection to fail to the secondary in less than one second.
What should be done to meet this requirement?

A. Configure BGP on the company’s router with a keep-alive to 300 ms and the BGP hold timer to 900 ms.
B. Enable Bidirectional Forwarding Detection (BFD) on the company’s router with a detection minimum interval of 300 ms and a BFD liveness detection multiplier of 3.
C. Enable Dead Peer Detection (DPD) on the company’s router with a detection minimum interval of 300 ms and a DPD liveliness detection multiplier of 3.
D. Enable Bidirectional Forwarding Detection (BFD) echo mode on the company’s router and disable sending the Internet Control Message Protocol (ICMP) IP packet requests.

Answer: B

NEW QUESTION 20
An organization will be expanding its current network design. When fully built out, there will be 99 VPCs spread across 11 AWS accounts (9 VPCs per account). There is currently an AWS Direct Connect connection into one account with 9 VPCs, each with a virtual network interface (VIF) per VPC.
Which of the following designs will minimize cost while allowing the organization to expand?

A. Order 10 new Direct Connect connections, one from each of the accounts that will be provisioned.Create private VIFs in each accoun
B. Attach one private VIF per VPC.
C. Create a public VIF on the Direct Connect connectio
D. Leverage the public VIF to create a VPN connection to each VPC.
E. Create hosted private VIFs in the existing accoun
F. Connect a private VIF to an AWS Direct Connect gateway in each accoun
G. Connect the gateway in each account to the VPCs.
H. Create a transit VPC in the existing account that consists of two routers in separate Availability Zones.Connect each VPC to the two routers in the transit VPC by using VPN.

Answer: D

Explanation:
https://docs.aws.amazon.com/directconnect/latest/UserGuide/limits.html

NEW QUESTION 22
A company has a hybrid IT architecture with two AWS Direct Connect connections to provide high availability. The services hosted on-premises are accessible using public IPs, and are also on the 172.16.0.0/16 range. The AWS resources are on the 192.168.0.0/18 range. The company wants to use Amazon Elastic Load Balancing for SSL offloading, health checks, and sticky sessions.
What should be done to meet these requirements?

A. Create a Network Load Balancer pointing to the on-premises server's private IP address.
B. Create an Amazon CloudFront distribution for the on-premises service and use the public IPs of the on-premises servers as the origin.
C. Create a Network Load Balancer pointing to the on-premises server's public IP address.
D. Create an Application Load Balancer pointing to the on-premises server's private IP address.

Answer: D

NEW QUESTION 25
A company wants to migrate its production and development applications to the AWS Cloud across multiple VPCs in three AWS Regions us-east-1 (N Virginia), eu-west-1 (Ireland), and ap-southeast-1 (Singapore) The company needs a scalable solution that provides connectivity between all three Regions The solution also must provide private connectivity to the company's on-premises data center in Northern Virginia Data that is transferred from on premises and data that is transferred between Regions must be encrypted in transit The company requires predictable network performance and must minimize cost
The company has initiated a solution by deploying a transit gateway with two route tables in each Region One route table is for the production environment, and one route table is for the development environment
What else must the company do to meet its requirements with the LOWEST latency?

A. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center On each transit gateway, create a VPN attachment over the public VIF for the production and development route tables Create transit gateway peennng connections to route traffic between Regions
B. Deploy an AWS Direct Connect connection in us-east-1 and a transit VIF to the on-premises data center Associate all transit gateways and the transit VIF with a different Direct Connect gatewa
C. Create transit gateway peering connections to route traffic between Regions
D. Deploy an AWS Direct Connect connection in us-east-1 and a public VIF to the on-premises data center.On each transit gateway, create a VPN attachment over the public VIF for the production and development route table
E. Route traffic between Regions through the VPN connections.
F. Deploy an AWS Direct Connect connection in us-east-1 to the on-premises data center Create one transit VIF for each transit gateway route table, and associate each transit VIF with a Direct Connect gateway Associate all transit gateways with the Direct Connect gateway Create transit gateway peering connections to route traffic between Regions.

Answer: B

NEW QUESTION 29
The Web Application Development team is worried about malicious activity from 200 random IP addresses. Which action will ensure security and scalability from this type of threat?

A. Use inbound security group rules to block the IP addresses.
B. Use inbound network ACL rules to block the IP addresses.
C. Use AWS WAF to block the IP addresses.
D. Write iptables rules on the instance to block the IP addresses.

Answer: C

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/amazon-vpc-limits.html

NEW QUESTION 32
You have a global corporate network with 153 individual IP prefixes in your internal routing table. You establish a private virtual interface over AWS Direct Connect to a VPC that has an Internet gateway (IGW). All instances in the VPC must be able to route to the Internet via an IGW and route to the global corporate network via the VGW.
How should you configure your on-premises BGP peer to meet these requirements?

A. Configure AS-Prepending on your BGP session
B. Summarize your prefix announcement to less than 100
C. Announce a default route to the VPC over the BGP session
D. Enable route propagation on the VPC route table

Answer: B

NEW QUESTION 33
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 35
You are designing the network infrastructure for an application server in Amazon VPC. Users will access all the application instances from the Internet and from an on-premises network. The on-premises network is connected to your VPC over an AWS Direct Connect link.
How should you design routing to meet these requirements?

A. Configure a single routing table with two default routes: one to the Internet via an IGW, the other to the on-premises network via the VG
B. Use this routing table across all subnets in your VPC.
C. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VG
D. Associate both routing tables with each VPC subnet.
E. Configure a single routing table with a default route via the IG
F. Propagate a default route via BGP on the AWS Direct Connect customer route
G. Associate the routing table with all VPC subnet.
H. Configure a single routing table with a default route via the IG
I. Propagate specific routes for theon-premises networks via BGP on the AWS Direct Connect customer route
J. Associate the routing table with all VPC subnets.

Answer: D

NEW QUESTION 38
An organization has multiple applications running in VPCs across multiple AWS accounts. The network engineer has deployed a central VPC with a pair of software VPN instances that run IPSec tunnels with dynamic routing to VGWs of all application VPCs. This central VPC is connected to on-premises resources via a Direct Connect connection using a private VIF.
What additional configuration is required to enable the applications in VPCs to communicate with each other and access on-premises resources?

A. Configure each application VPC with a static route entry pointing the on-premises CIDR block to the software VPN instances.
B. Configure the central VPC with a static route entry pointing the on-premises CIDR block to local VGWs.
C. Advertise all application VPC CIDR blocks to on-premises resources via the VGW in the central VPC.
D. Configure IPSec tunnels from the on-premises router into the software VPN instances with dynamic routing.

Answer: D

NEW QUESTION 39
A multinational organization has applications deployed in three different AWS regions. These applications must securely communicate with each other by VPN.
According to the organization’s security team, the VPN must meet the following requirements:
AES 128-bit encryption
SHA-1 hashing
User access via SSL VPN
PFS using DH Group 2
Ability to maintain/rotate keys and passwords
Certificate-based authentication
Which solution should you recommend so that the organization meets the requirements?

A. AWS hardware VPN between the virtual private gateway and customer gateway
B. A third-party VPN solution deployed from AWS Marketplace
C. A private MPLS solution from an international carrier
D. AWS hardware VPN between the virtual private gateways in each region

Answer: B

Explanation:
https://blog.cloudthat.com/configuring-vpn-between-the-vpcs-across-regionsaccounts/

NEW QUESTION 41
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 43
A company is building a hybrid PCI-DSS compliant application that runs in the us-west-2 Region and
on-premises. The application sends access logs from all locations to a single Amazon S3 bucket in us-west-2 To protect this sensitive data, the bucket policy is configured to deny access from public IP addresses
How should an engineer configure the network to meet these requirements?

A. Configure an AWS Direct Connect private virtual interface to the company's AWS VPC in us-west-2 Create a VPC endpoint and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3
B. Configure a VPN connection to the company's AWS VPC in us-west-2 and use BGP to advertise routes for Amazon S3
C. Configure a Direct Connect connection public virtual interface to us-west-2 Leverage an on-premises HTTPS proxy to send traffic to Amazon S3 over a Direct Connect connection

D. Configure a VPN connection to the company's AWS VPC in us-west-2 Create a NAT gateway and configure the on-premises systems to leverage an HTTPS proxy in the VPC to access Amazon S3

Answer: C

NEW QUESTION 47
A computing team is evaluating whether to place a high performance computing (HPC) application in AWS. The team is concerned about application performance and wants to know what options are available to increase networking performance.
Which of the following changes would increase performance for this application? (Choose two.)

A. Place the application across many smaller instances to achieve higher total throughput.
B. Increase the MTU of the VPC to 9001.
C. Enable an MTU of 9001 in the application's operating system.
D. Enable enhanced networking on the instances.
E. Deploy the application in two Availability Zones and insert them in one placement group.

Answer: CD

NEW QUESTION 49
A company's developers wrote an AWS Lambda function to modify existing private route tables in response to a security appliance's auto scaling events. The Lambda function will be invoked on lifecycle hooks for an Auto Scaling group and Is configured to run in a VPC The developers are unsure if the following 1AM policy provides sufficient permissions to be used as an execution role for this Lambda function.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "ec2:CreateRoute",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssignPrivateIpAddresses",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

The developers ask a network engineer to review the permissions.
Which set of permissions should the network engineer add lo the policy?

A. lambd
B. ListFunctions, lambda:GetPolicy, and ec2 Delete RouteTable
C. ec2:AssociateAddress, ec2 ModifylnstanceAttribut
D. and ec2 AssociateRouteTable
E. ec2:CreateNetworklntertace ec2 DeleteNetworklnterface, and ec2 ReplaceRoute
F. ec2:Describei.ifecydoHooks, ec2 DescribeScalingActivities, and ec2 DescribePolicies

Answer: C

NEW QUESTION 50
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 54
You need to set up an Amazon Elastic Compute Cloud (EC2) instance for an application that requires the lowest latency and the highest packet-per-second network performance. The application will talk to other servers in a peered VPC.
Which two of the following components should be part of the design? (Select two.)

A. Select an instance with support for single root I/O virtualization.
B. Select an instance that has support for multiple ENIs.
C. Ensure that the instance supports jumbo frames and set 9001 MTU.
D. Select an instance with Amazon Elastic Block Store (EBS)-optimization.
E. Ensure that proper OS drivers are installed.

Answer: AE

Explanation:
References: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

NEW QUESTION 56
Changes made to a security group attached to an Application Load Balancer resulted in connectivity issues for a company's production web application. The Network Engineer needs to lock down permissions for the company's AWS account, automate auditing for any changes, and set up notifications.
What actions should accomplish this?

A. Configure IAM user policies to lock down permissions for specific user
B. Enable AWS CloudTrail to identify API calls from user
C. Use AWS Config to audit any changes, and configure Amazon SNS to send notifications.
D. Configure IAM user policies to lock down permissions for specific user
E. Enable AWS CloudTrail to identify the API calls from user
F. Configure AWS CodeCommit to audit any changes in configurations, and configure Amazon SNS to send notifications.
G. Configure IAM user policies to lock down permissions for specific user
H. Enable AWS CloudTrail to identify the API calls from user
I. Configure Amazon Macie to use machine learning to identify any configuration changes, and configure Amazon SNS to send notifications.
J. Configure IAM role policies to lock down permissions for specific user
K. Configure Amazon GuardDuty to audit and monitor configuration changes, and configure Amazon SNS to send notifications.

Answer: A

NEW QUESTION 59
A customer has set up multiple VPCs for Dev, Test, Prod, and Management. You need to set up AWS Direct Connect to enable data flow from on-premises to each VPC. The customer has monitoring software running in the Management VPC that collects metrics from the instances in all the other VPCs. Due to budget requirements, data transfer charges should be kept at minimum.
Which design should be recommended?

A. Create a total of four private VIFs, one for each VPC owned by the customer, and route traffic between VPCs using the Direct Connect link.
B. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs.
C. Create a private VIF to the Management VPC, and peer this VPC to all other VPCs, enable source/destination NAT in the Management VPC.
D. Create a total of four private VIFs, and enable VPC peering between all VPCs.

Answer: A

NEW QUESTION 63
All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

A. The NAT gateway does not support UDP traffic.
B. The authentication server is not accepting traffic.
C. The NAT gateway cannot allocate more ports.
D. The NAT gateway is launched in a private subnet.

Answer: C

Explanation:
Ref: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
"A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon CloudWatch."

NEW QUESTION 64
An organization processes consumer information submitted through its website. The organization’s security policy requires that personally identifiable information (PII) elements are specifically encrypted at all times and as soon as feasible when received. The front-end Amazon EC2 instances should not have access to decrypted PII. A single service within the production VPC must decrypt the PII by leveraging an iAM role.
Which combination of services will support these requirement? (Select two.)

A. Amazon Aurora in a private subnet
B. Amazon CloudFront using AWS Lambda@Edge
C. Customer-managed MySQL with Transparent Data Encryption
D. Application Load Balancer using HTTPS listeners and targets
E. AWS Key Management Services

Answer: BE

NEW QUESTION 68
A company deployed its production Amazon VPC using CIDR block 33.16.0.0/16. The company has nearly depleted its addresses and now needs to extend the VPC network.
Which CIDR blocks meet the company’s requirement to extend the VPC network with a secondary CIDR? (Choose two.)

A. 33.17.0.0/16
B. 172.16.0.0/18
C. 100.70.0.0/17
D. 192.168.1.0/24
E. 10.0.0.0/8

Answer: AC

NEW QUESTION 69
A company needs to allow its remote users to access company resources in the AWS Cloud. The company has two VPCs that are connected through VPC peering. The remote users must be able to access resources in both VPCs by using secure connections from their laptop computers The company does not want to implement an access management solution that requires additional costs or effort.
Which solution meets these requirements?

A. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target networ
B. Add a rule to authorize client access to the target VP
C. and add a rule to authorize client access to the peered VP
D. Update resource security groups in both VPCs to allow traffic from the security group for the subnet associatio
E. Instruct the users to sign in to the AWS Management Console and navigate to Client VPN to connect to the Client VPN endpoint.
F. Deploy an AWS Client VPN endpoint in both VPCs, associate subnets, and define a target networ
G. Add a rule to authorize client access to each target VP
H. Update resource security groups in both VPCs to allow traffic from the security groups of each VPC for the subnet association
I. Securely send the users the configuration options, and instruct the users to install Client VPN endpoints at the same time to gain access to the resources.
J. Deploy a Network Load Balancer in front of the company resource
K. Set up security groups that contain the IP addresses of each of the user laptop
L. Instruct the users to connect to the application securely over TCP.
M. Deploy an AWS Client VPN endpoint in one VPC, associate a subnet, and define a target networ
N. Add a rule to authorize client access to the target VP
O. and add a rule to authorize client access to the peered VP
P. Update resource security groups in both VPCs to allow traffic from the security group for the subnet associatio
Q. Securely send the users the configuration options, and instruct the users to install Client VPN on their laptop
R. Instruct the users to connect to the Client VPN endpoint to gain access to the resources.

Answer: B

NEW QUESTION 74
A company has applications running in a single AWS Region and its on premises data center in a hybrid mode The company has a 1Gbps AWS Direct Connect connection from the data center to AWS that is 65% utilized. The company has an AWS Enterprise Support plan
The company is planning to deploy a new critical application on AWS that will connect with existing applications running in the data center. The application SLA requires a minimum ot 99.9% network uptime between the data center and AWS.
What is the MOST cost-effective way to meet this SLA requirement?

A. Create a second virtual interface (VIF) on the existing Direct Connect connection, and terminate this VIF in the existing VPC Use BGP for load balancing between the VIFs in active/active mode.
B. Purchase an additional 1Gbps Direct Connect connection from AWS In a different cross-connect location terminated in the associated Region Provision a new virtual interface (VIF) to the existing VP
C. and use BGP for load balancing
D. Set up two new hosted Direct Connect connections of 500 Mbps each through an AWS Direct Connect partne
E. Provision two virtual interfaces (VIFs) to the existing VPC on both Direct Connect connections, and use BGP for load balancing Terminate the existing 1Gbps Direct Connect connection
F. Purchase an additional 1Gbps Direct Connect connection from AWS in the existing cross-connect location Ask AWS to terminate this new connection in a different router Provision two virtual interfaces (VIFs) to the same VPC on both Direct Connect connections, and use BGP for load balancing

Answer: A

NEW QUESTION 77
Your company operates a single AWS account. A common services VPC is deployed to provide shared services, such as network scanning and compliance tools. Each AWS workload uses its own VPC, and each VPC must peer with the common services VPC. You must choose the most efficient and cost effective approach.
Which approach should be used to automate the required VPC peering?

A. AWS CloudTrail integration with Amazon CloudWatch Logs to trigger a Lambda function.
B. An OpsWorks Chef recipe to execute a command-line peering request.
C. Cfn-init with AWS CloudFormation to execute a command-line peering request.
D. An AWS CloudFormation template that includes a peering request.

Answer: D

Explanation:
https://cloakable.irdeto.com/2017/10/11/how-to-implement-vpc-peering-between-2-vpcs-in-the-same-aws-accou

NEW QUESTION 81
Your company uses an NTP server to synchronize time across systems. The company runs multiple versions of Linux and Windows systems. You discover that the NTP server has failed, and you need to add an alternate NTP server to your instances.
Where should you apply the NTP server update to propagate information without rebooting your running instances?

A. DHCP Options Set
B. instance user-data
C. cfn-init scripts
D. instance meta-data

Answer: A

Explanation:
https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-dhcp-options.html

NEW QUESTION 86

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.

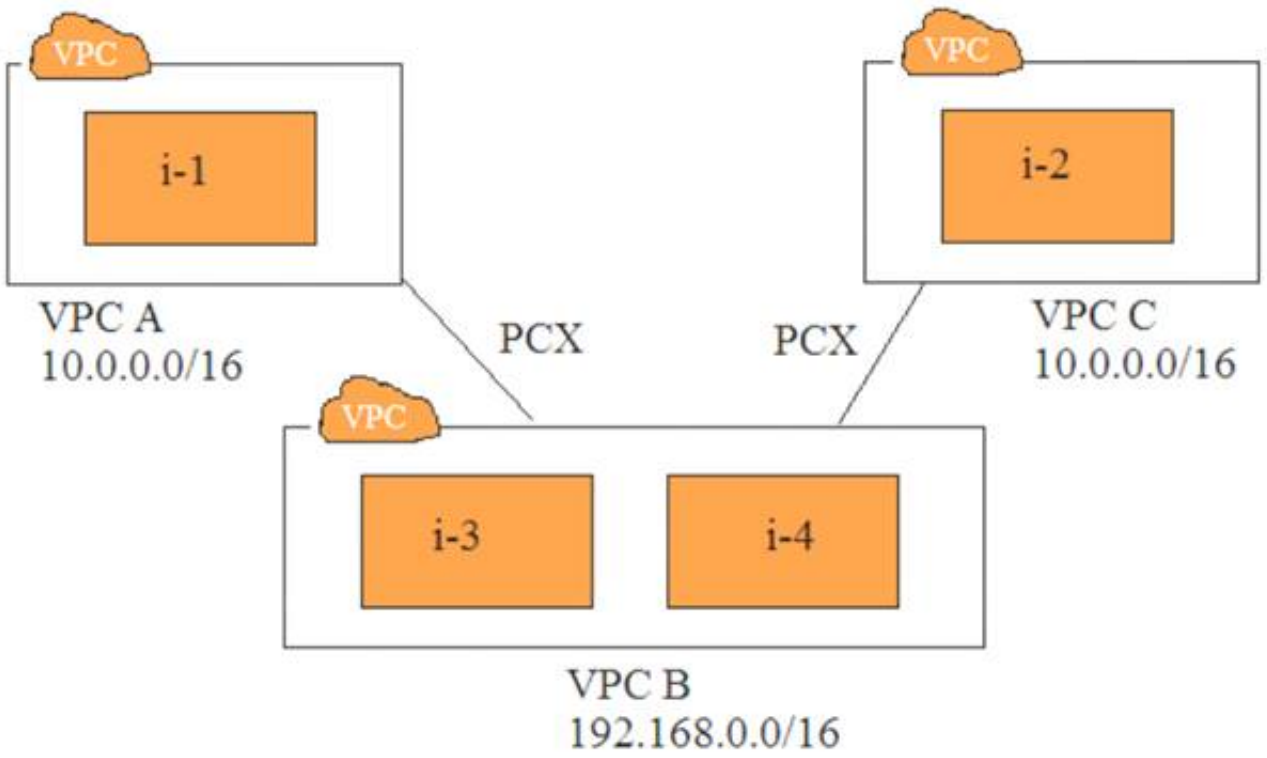
Answer: D

NEW QUESTION 89
A Network Engineer needs to be automatically notified when a certain TCP port is accessed on a fleet of Amazon EC2 instances running in an Amazon VPC.
Which of the following is the MOST reliable solution?

A. Create an inbound rule in the VPC's network ACL that matches the TCP por
B. Create an Amazon CloudWatch alarm on the NetworkPackets metric for the ACL that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
C. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to notify the Administrator with Amazon SNS each time the TCP port is accessed.
D. Create VPC Flow Logs that write to Amazon CloudWatch Logs, with a metric filter matching connections on the required por
E. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.
F. Install intrusion detection software on each Amazon EC2 instance and configure it to use the AWS CLI to publish to a custom Amazon CloudWatch metric each time the TCP port is accesse
G. Create a CloudWatch alarm on the resulting metric that uses Amazon SNS to notify the Administrator when the metric is greater than zero.

Answer: A

NEW QUESTION 90
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 92
You use a VPN to extend your corporate network into a VPC. Instances in the VPC are able to resolve resource records in an Amazon Route 53 private hosted zone. Your on-premises DNS server is configured with a forwarder to the VPC DNS server IP address. On-premises users are unable to resolve names in the private hosted zone, although instances in a peered VPC can.

What should you do to provide on-premises users with access to the private hosted zone?

A. Create a proxy resolver within the VP
B. Point the on-premises forwarder to the proxy resolver.
C. Modify the network access control list on the VPC to allow DNS queries from on-premises systems.
D. Configure the on-premises server as a secondary DNS for the private zon
E. Update the NS records.
F. Update the on-premises forwarders with the four name servers assigned to the private hosted zone.

Answer: A

Explanation:
References:
https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-b

NEW QUESTION 95
Under increased cybersecurity concerns, a company is deploying a near real-time intrusion detection system (IDS) solution. A system must be put in place as soon as possible. The architecture consists of many AWS accounts, and all results must be delivered to a central location.
Which solution will meet this requirement, while minimizing downtime and costs?

A. Deploy a third-party vendor solution to perform deep packet inspection in a transit VPC.
B. Enable VPC Flow Logs on each VP
C. Set up a stream of the flow logs to a central Amazon Elasticsearch cluster.
D. Enable Amazon Macie on each AWS account and configure central reporting.
E. Enable Amazon GuardDuty on each account as members of a central account.

Answer: D

Explanation:
References:
https://aws.amazon.com/blogs/security/how-to-manage-amazon-guardduty-security-findings-across-multiple-acc

NEW QUESTION 97
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 99
A company has an AWS Direct Connect connection between its on-premises data center and Amazon VPC. An application running on an Amazon EC2 instance in the VPC needs to access confidential data stored in the on-premises data center with consistent performance For compliance purposes, data encryption is required.
What should the network engineer do to meet these requirements?

A. Configure a public virtual interface on the Direct Connect connectio
B. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
C. Configure a private virtual interface on the Direct Connect connectio
D. Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.
E. Configure an internet gateway in the VPC Set up a software VPN between the customer gateway and an EC2 instance in the VPC.
F. Configure an internet gateway in the VPC Set up an AWS Site-to-Site VPN between the customer gateway and the virtual private gateway in the VPC.

Answer: D

NEW QUESTION 100
A company installed an AWS Site-to-Site VPN and configured it to use two tunnels The company has learned that the VPN connectivity is unstable During a ping test from the on-premises data center to AWS: a network engineer notices that the first few ICMP replies time out but that subsequent requests are successful The AWS Management Console shows that the status for both tunnels last changed at the same time the ping responses were successfully received
Which steps should the network engineer take to resolve the instability*? (Select TWO)

A. Enable dead peer detection (DPD) on the customer gateway device
B. Change the tunnel configuration to active/standby on the virtual private gateway
C. Use AS PATH prepending on one path to cause all traffic to prefer that tunnel
D. Send ICMP requests to an instance in the VPC every 5 seconds from the on-premises network
E. Use a higher multi-exit discriminator (MED) value on the preferred path to prefer that tunnel

Answer: CE

NEW QUESTION 102

A company has 225 mobile and desktop devices and 300 partner VPNs that need access to an AWS VPC. VPN users should not be able to reach one another.
Which approach will meet the technical and security requirements while minimizing costs?

A. Use the AWS IPsec VPN for the mobile, desktop, and partner VPN connection
B. Use network access control lists (Network ACLs) and security groups to maintain routing separation.
C. Use the AWS IPsec VPN for the partner VPN connection
D. Use an Amazon EC2 instance VPN for the mobile and desktop device
E. Use Network ACLs and security groups to maintain routing separation.
F. Create an AWS Direct Connect connection between on-premises and AWS Use a public virtual interface to connect to the AWS IPsec VPN for the mobile, desktop, and partner VPN connections.
G. Use an Amazon EC2 instance VPN for the desktop, mobile, and partner VPN connection
H. Use features of the VPN instance to limit routing and connectivity.

Answer: D

NEW QUESTION 105
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.
What are the minimum requirements for your router?

A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
C. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
D. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel

Answer: B

NEW QUESTION 110
A team implements a highly available solution using Amazon AppStream 2.0. The AppStream 2.0 fleet needs to communicate with resources both in an existing VPC and on-premises. The VPC is connected to the on-premises environment using an AWS Direct Connect private virtual interface.
What implementation enables on-premises users to connect to AppStream and existing VPC resources?

A. Deploy two subnets into the existing VP
B. Add a public virtual interface to the Direct Connect connection for users to access the AppStream endpoint
C. Deploy two subnets into the existing VP
D. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.
E. Deploy a new VPC with two subnet
F. Create a VPC peering connection between the two VPCs for users to access the AppStream endpoint.
G. Deploy one subnet into the existing VP
H. Add a private virtual interface on the Direct Connect connection for users to access the AppStream endpoint.

Answer: B

NEW QUESTION 114
You currently use a single security group assigned to all nodes in a clustered NoSQL database. Only your cluster members in one region must be able to connect to each other. This security group uses a
self-referencing rule using the cluster security group's group-id to make it easier to add or remove nodes from the cluster. You need to make this database comply with out-of-region disaster recovery requirements and ensure that the network traffic between the nodes is encrypted when travelling between regions. How should you enable secure cluster communication while deploying additional cluster members in another AWS region?

A. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group rules that reference each other's security group-id in each region.
B. Create an IPsec VPN between AWS regions, use private IP addresses to route traffic, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
C. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group CIDR-based rules that correspond with the VPC CIDR in the other region.
D. Use public IP addresses and TLS to securely communicate between cluster nodes in each AWS region, and create cluster security group rules that reference each other's security group-id in each region.

Answer: B

NEW QUESTION 118
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 120
An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.
Which solution will fix the connectivity failures with the LEAST amount of effort?

A. Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.
B. Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route tableAPIs.
C. Update the application server's outbound security group to use the prefix-list for Amazon S3 in the same region.
D. Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer: C

Explanation:
https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

NEW QUESTION 123
A Lambda function needs to access the private address of an Amazon ElastiCache cluster in a VPC. The Lambda function also needs to write messages to Amazon SQS. The Lambda function has been configured to run in a subnet in the VPC.
Which of the following actions meet the requirements? (Select two.)

A. The Lambda function needs an IAM role to access Amazon SQS
B. The Lambda function must route through a NAT gateway or NAT instance in another subnet to access the public SQS API.
C. The Lambda function must be assigned a public IP address to access the public Amazon SQS API.
D. The ElastiCache server outbound security group rules must be configured to permit the Lambda function's security group.
E. The Lambda function must consume auto-assigned public IP addresses but not elastic IP addresses.

Answer: AB

Explanation:
https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html https://docs.aws.amazon.com/lambda/latest/dg/vpc.html

NEW QUESTION 128
You operate a production VPC with both a public and a private subnet. Your organization maintains a restricted Amazon S3 bucket to support this production workload. Only Amazon EC2 instances in the private subnet should access the bucket. You implement VPC endpoints(VPC-E) for Amazon S3 and remove the NAT that previously provided a network path to Amazon S3. The default VPC-E policy is applied. Neither EC2 instances in the public or private subnets are able to access the S3 bucket.
What should you do to enable Amazon S3 access from EC2 instances in the private subnet?

A. Add the CIDR address range of the private subnet to the S3 bucket policy.
B. Add the VPC-E identified to the S3 bucket policy.
C. Add the VPC identifier for the production VPC to the S3 bucket policy.
D. Add the VPC-E identifier for the production VPC to endpoint policy.

Answer: B

Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-endpoints-s3.html#vpc-endpoints-policies-s3

NEW QUESTION 131
You need to set up a VPN between AWS VPC and your on-premises network. You create a VPN connection in the AWS Management Console, download the configuration file, and install it on your on-premises router. The tunnel is not coming up because of firewall restrictions on your router. Which two network traffic options should you allow through the firewall? (Select two.)

A. UDP port 500
B. IP protocol 50
C. IP protocol 5
D. TCP port 50
E. TCP port 500

Answer: AB

Explanation:
References: https://docs.aws.amazon.com/vpc/latest/userguide/VPC_VPN.html

NEW QUESTION 134
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

AWS-Certified-Advanced-Networking-Specialty Practice Exam Features:

* AWS-Certified-Advanced-Networking-Specialty Questions and Answers Updated Frequently

* AWS-Certified-Advanced-Networking-Specialty Practice Questions Verified by Expert Senior Certified Staff

* AWS-Certified-Advanced-Networking-Specialty Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* AWS-Certified-Advanced-Networking-Specialty Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year