Question: 1

Your organization's corporate website must be available on www.acme.com and acme.com.
How should you configure Amazon Route 53 to meet this requirement?

A. Configure acme.com with an ALIAS record targeting the ELB. www.acme.com with an ALIAS record targeting the ELB.
B. Configure acme.com with an A record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
C. Configure acme.com with a CNAME record targeting the ELB. www.acme.com with a CNAME record targeting the acme.com record.
D. Configure acme.com using a second ALIAS record with the ELB target. www.acme.com using a PTR record with the acme.com record target.

Answer: A

Explanation:

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-elb-load-balancer.html

Question: 2

You are building an application in AWS that requires Amazon Elastic MapReduce (Amazon EMR). The application needs to resolve hostnames in your internal, on-premises Active Directory domain. You update your DHCP Options Set in the VPC to point to a pair of Active Directory integrated DNS servers running in your VPC.

Which action is required to support a successful Amazon EMR cluster launch?

A. Add a conditional forwarder to the Amazon-provided DNS server.
B. Enable seamless domain join for the Amazon EMR cluster.
C. Launch an AD connector for the internal domain.
D. Configure an Amazon Route 53 private zone for the EMR cluster.

Answer: A

Explanation:

https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-using-aws-directory-service-and-microsoft-active-directory/

Question: 3

You have a three-tier web application with separate subnets for Web, Applications, and Database tiers. Your CISO suspects your application will be the target of malicious activity. You are tasked with notifying the security team in the event your application is port scanned by external systems.

Which two AWS Services cloud you leverage to build an automated notification system? (Select two.)

A. Internet gateway
B. VPC Flow Logs
C. AWS CloudTrail
D. Lambda
E. AWS Inspector

Answer: BD

Explanation:

Reference: https://aws.amazon.com/blogs/security/how-to-receive-alerts-when-specific-apis-are-called-by-using-aws-cloudtrail-amazon-sns-and-aws-lambda/

Question: 4

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 VGW. Use this routing table across all subnets in your VPC.
B. Configure two routing tables: one that has a default route via the IGW, and another that has a default route via the VGW. Associate both routing tables with each VPC subnet.
C. Configure a single routing table with a default route via the IGW. Propagate a default route via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnet.
D. Configure a single routing table with a default route via the IGW. Propagate specific routes for the on-premises networks via BGP on the AWS Direct Connect customer router. Associate the routing table with all VPC subnets.

Answer: D

Explanation:

0/0 to IGW and advertise specific routes or (10/8) from onprem to VGW and propogate to VPC

Question: 5

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/

Question: 6

Your organization uses a VPN to connect to your VPC but must upgrade to a 1-G AWS Direct Connect connection for stability and performance. Your telecommunications provider has provisioned the circuit from your data center to an AWS Direct Connect facility and needs information on how to cross-connect (e.g., which rack/port to connect).

What is the AWS-recommended procedure for providing this information?

A. Create a support ticket. Provide your AWS account number and telecommunications company's name and where you need the Direct Connect connection to terminate.
B. Create a new connection through your AWS Management Console and wait for an email from AWS with information.
C. Ask your telecommunications provider to contact AWS through an AWS Partner Channel. Provide your AWS account number.
D. Contact an AWS Account Manager and provide your AWS account number, telecommunications company's name, and where you need the Direct Connect connection to terminate.

Answer: B

Explanation:

https://aws.amazon.com/premiumsupport/knowledge-center/provision-direct-connection/
https://docs.aws.amazon.com/directconnect/latest/UserGuide/getting_started.html

Question: 7

You manage a web service that is used by client applications deployed in 300 offices worldwide. The web service architecture is an Elastic Load balancer (ELB) distributing traffic across four application servers deployed in an autoscaling group across two availability zones.

The ELB is configured to use round robin, and sticky sessions are disabled. You have configured the NACLs and Security Groups to allow port 22 from your bastion host, and port 80 from 0.0.0.0/0. The client configuration is managed by each regional IT team.

Upon inspection you find that a large amount of requests from incorrectly configured sites are causing a single application server to degrade. The remainder of the requests are equally distributed across all servers with no negative effects.

What should you do to remedy the situation and prevent future occurrences?

A. Mark the affected instance as degraded in the ELB and raise it with the client application team.
B. Update the NACL to only allow port 80 to the application servers from the ELB servers.
C. Update the Security Groups to only allow port 80 to the application servers from the ELB.
D. Terminate the affected instance and allow Auto Scaling to create a new instance.

Answer: C

Explanation:

IT guy might route the clients app from one or some offices directly to web service instead of ELB IP address. So C. Configure the application servers SG only accept the connection with port 80 from ELB is correct. It will block all other traffic from another source IP, in this case from client applications. Then avoid such issue.

Question: 8

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

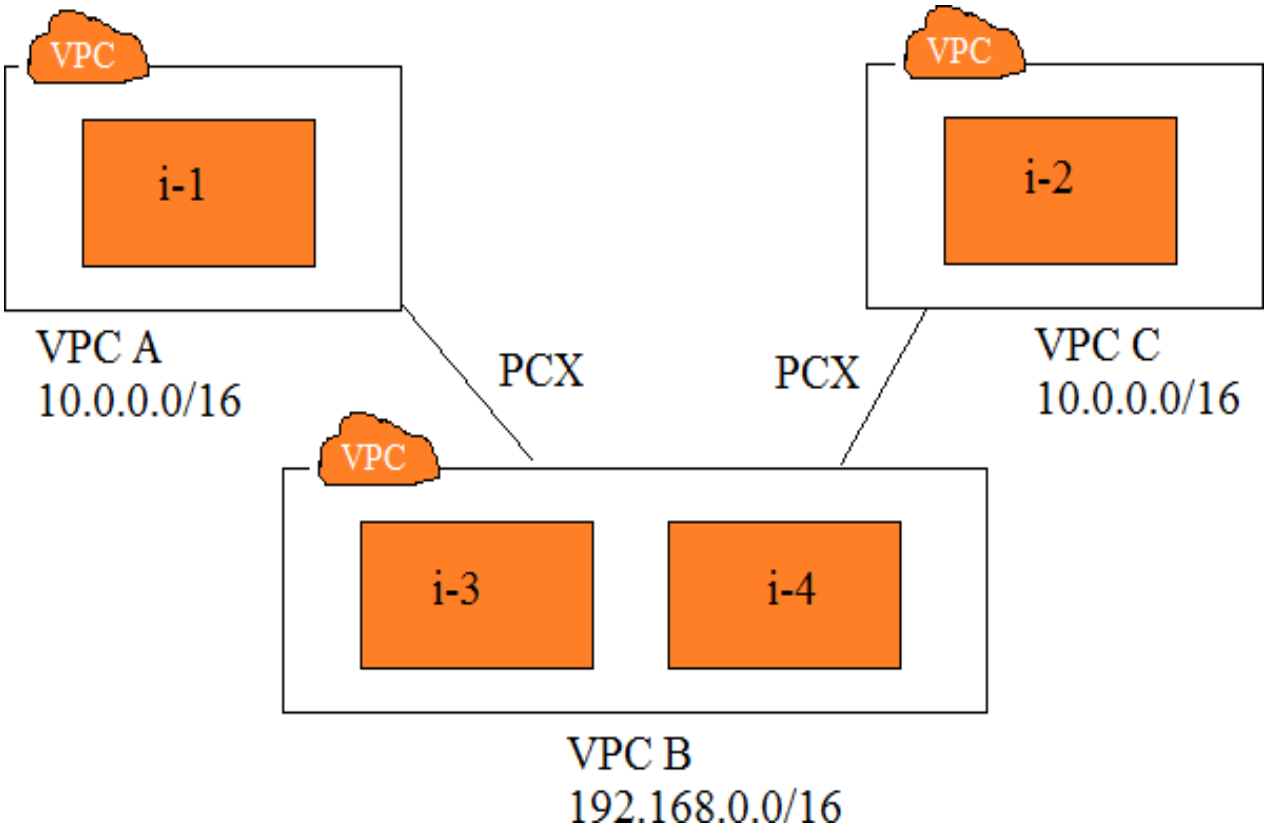
Answer: B

Explanation:

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

Question: 9

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-simple-hub

Question: 10

A legacy, on-premises web application cannot be load balances effectively. There are both planned and unplanned events that cause usage spikes to millions of concurrent users. The existing infrastructure cannot handle the usage spikes. The CIO has mandated that the application be moved to the cloud to avoid further disruptions, with the additional requirement that source IP addresses be unaltered to support network traffic-monitoring needs. Which of the following designs will meet these requirements?

A. Use an Auto Scaling group of Amazon EC2 instances behind a Classic Load Balancer.
B. Use an Auto Scaling group of EC2 instances in a target group behind an Application Load Balancer.
C. Use an Auto Scaling group of EC2 instances in a target group behind a Classic Load Balancer.
D. Use an Auto Scaling group of EC2 instances in a target group behind a Network Load Balancer.

Answer: D