🏠 (https://www.whizlabs.com/learn) › My Courses (https://www.whizlabs.com/learn/my-courses)
› AWS Certified Advanced Networking Specialty (https://www.whizlabs.com/learn/course/aws-cans-practice-tests#section-1)
› New Practice Test II (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14783) › Report

NEW PRACTICE TEST II

Attempt	1	**Completed on**	Sunday , 03 February 2019 , 12:24 AM
Marks Obtained	1 / 65	**Time Taken**	00 H 00 M 13 S
Your score is	1.54%	**Result**	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Design and implement AWS networks	13	0	1	12
2	Manage, optimize, and troubleshoot the network	13	0	0	13
3	Automate AWS tasks	3	0	0	3
4	Design and implement for security and compliance	16	1	0	15
5	Design and implement hybrid IT network architectures at scale	11	0	0	11
6	Configure network integration with application services	9	0	0	9

65	**1**	**1**	**63**
Questions	Correct	Incorrect	Unattempted

Show Answers All

QUESTION 1 INCORRECT DESIGN AND IMPLEMENT AWS NETWORKS

You have a MySQL cluster which is hosted in AWS. The nodes in the cluster currently work with the private IP addresses. There is a self-referencing security group which is used for securing access across the nodes of the cluster. There is now a requirement to ensure disaster recovery for these nodes in another region. How can you achieve communication across the nodes in different regions securely?

○ **A.** Use public IP addresses and use SSL certificates for secure communication across the nodes.

○ **B.** Use the private IP addresses of the nodes and use SSL certificates for secure communication across the nodes ✖

○ **C.** Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the security groups assigned to the nodes in the primary region

○ **D.** Create a VPN IPSec tunnel. Ensure the nodes in the different region reference the VPC CIDR block in their security groups ✔

Explanation :

Answer – D

You need to use a VPN IPSec tunnel for secure communication across the Internet between the regions.

Option A is invalid because public IP addresses via the Internet is not a secure way for communication

Option B is invalid because private IP addresses are not routable via the Internet

Option C is invalid because the same security groups cannot be accessed across regions

For more information on VPN connections , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html)

Ask our Experts

QUESTION 2 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company has a department that has set their own AWS account that is not part of the consolidating billing process for the company. They have setup a AWS Direct connect connection to a VPC via a Private VIF. They are downloading data from an EC2 Instance in the VPC. How would the charges come across?

○ **A.** The company would be charged for data transfer out via the Internet gateway

○ **B.** The company would be charged for data transfer out via AWS Direct Connect

○ **C.** The department would be charged for data transfer out via the Internet gateway

○ **D.** The department would be charged for data transfer out via AWS Direct Connect ✔

Explanation :

Answer – D

Since the department have opened the AWS account irrespective of the company , they would be charged. They would be charged on the Data transfer out.

The below excerpt from the AWS Documentation shows the data transfer charges

AWS Direct Connect data transfer

Data transfer IN is $0.00 per GB in all locations.

Data Transfer OUT pricing is dependent on the source AWS Region and AWS Direct Connect location. Please choose your Direct Connect location from the relevant section below to get $/GB pricing for Data Transfer Out from AWS Region to AWS Direct Connect location, or click here for full data transfer pricing table.

For more information on AWS Direct Connect billing, please refer to the below URL

- https://aws.amazon.com/directconnect/pricing/ (https://aws.amazon.com/directconnect/pricing/)

Ask our Experts 👍 👎

QUESTION 3 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have setup an EC2 Instance that hosts a web application. You have set the following rules

- Security Group Rules
  - Allow Inbound Traffic on port 80 from 0.0.0.0/0
  - Deny Outgoing Traffic
- NACL
  - Allow Inbound Traffic on port 80 from 0.0.0.0/0
  - Deny Outgoing Traffic

Users are complaining that they cannot access the web server. How can you ensure that the issue gets resolved?

○ **A.** Allow Outgoing Traffic on the Security groups for port 80

○ **B.** Allow Outgoing Traffic on the NACL for port 80

○ **C.** Allow Outgoing Traffic on the Security groups for ephemeral ports

○ **D.** Allow Outgoing Traffic on the NACL for ephemeral ports ✓

Explanation :

Answer – D
This is also given in the AWS Documentation
The client that initiates the request chooses the ephemeral port range. The range varies depending on the client's operating system. Many Linux kernels (including the Amazon Linux kernel) use ports 32768-61000. Requests originating from Elastic Load Balancing use ports 1024-65535. Windows operating systems through Windows Server 2003 use ports 1025-5000. Windows Server 2008 and later versions use ports 49152-65535. A NAT gateway uses ports 1024-65535. For example, if a request comes into a web server in your VPC from a Windows XP client on the Internet, your network ACL must have an outbound rule to enable traffic destined for ports 1025-5000.
Options A and C are incorrect since Security groups are stateful and hence you don't need to open the outbound rules here
Option B is incorrect since only the incoming traffic should accept port 80
For more information on ephemeral ports , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#VPC_ACLs_Ephemeral_Port (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html#VPC_ACLs_Ephemeral_Ports)

Ask our Experts 👍 👎

QUESTION 4 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on opening an AWS Direct Connect connection. They need to ensure that their router has the required capabilities to support this connection. Which of the following needs to be supported by the router. Choose 3 answers from the options given below

□ **A.** Single Mode Fibre ✓

□ **B.** 1 Gpbs copper connection

□ **C.** 802.1Q VLAN ✓

□ **D.** BGP and BGP MD5 authentication ✓

□ **E.** 802.1ad

Explanation :

Answer – A,C and D

Options B and E are incorrect since the requirements are clearly mentioned in the documentation

The AWS Documentation mentions the following on what needs to be supported

- Your network must use single mode fiber with a 1000BASE-LX (1310nm) transceiver for 1 gigabit Ethernet, or a 10GBASE-LR (1310nm) transceiver for 10 gigabit Ethernet.
- Auto-negotiation for the port must be disabled. Port speed and full-duplex mode must be configured manually.
- 802.1Q VLAN encapsulation must be supported across the entire connection, including intermediate devices.
- Your device must support Border Gateway Protocol (BGP) and BGP MD5 authentication.
- (Optional) You can configure Bidirectional Forwarding Detection (BFD) on your network.

Asynchronous BFD is automatically enabled for AWS Direct Connect virtual interfaces, but will not take effect until you configure it on your router.

For more information on AWS Direct Connect , please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Welcome.html)

Ask our Experts 👍 👎

QUESTION 5 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company has an AWS Direct connect connection in the us-west region. They are currently using a public VIF to access an S3 bucket in the us-west region. They now want to make use of AWS Direct Connect to access an S3 bucket in the us-east region. How can this be achieved in the most economical way?

○ **A.** Create another AWS Direct connect connection from your on-premise network in the us-east region.

○ **B.** Create another Private VIF from your current AWS Direct connect connection

○ **C.** Create another Public VIF from your current AWS Direct connect connection ✓

○ **D.** Create an VPN IPsec connection

Explanation :

Answer – C

The AWS Documentation mentions the following to support this

AWS Direct Connect locations in public regions or AWS GovCloud (US) can access public services in any other public region (excluding China (Beijing)). In addition, AWS Direct Connect connections in public regions or AWS GovCloud (US) can be configured to access a VPC in your account in any other public region (excluding China (Beijing)). You can therefore use a single AWS Direct Connect connection to build multi-region services. All networking traffic remains on the AWS global network backbone, regardless of whether you access public AWS services or a VPC in another region.

Option A is possible , but is not the most economical route

Option B is incorrect since a Private VIF cannot be used for public resources

Option D is incorrect since you can make use of the current AWS Direct Connect connection

For more information on AWS Direct Connect Remote regions, please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html)

Ask our Experts

QUESTION 6 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company has an AWS Direct connect connection in the us-west region. They want to use a VPC via the AWS Direct Connect connection. The VPC is located in another region. How can you achieve this connectivity? Choose 2 answers from the options given below.

□ **A.** Create a private VIF from the current AWS Direct Connect Connection. With Inter-region peering this is possible.

□ **B.** Create a Direct Connect gateway in a public region ✓

□ **C.** Create a Public VIF and then a VPN connection over that to the remote VPC ✓

□ **D.** Create a private VIF and then a VPN connection over that to the remote VPC

Explanation :

Answer – B and C

The AWS Documentation mentions the following

You can create a Direct Connect gateway in any public region and use it to connect your AWS Direct Connect connection over a private virtual interface to VPCs in your account that are located in different regions.
Alternatively, you can create a public virtual interface for your AWS Direct Connect connection and then establish a VPN connection to your VPC in the remote region
Option A and D are incorrect because using a private VIF will not help the requirement
For more information on AWS Direct Connect Remote regions, please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/remote_regions.html)

Ask our Experts 👍 👎

QUESTION 7 UNATTEMPTED AUTOMATE AWS TASKS

You need to perform a deep packet analysis for packets that are being sent to your EC2 Instance. Which of the following can help you accomplish this?

○ **A.** Wireshark ✓

○ **B.** AWS CloudTrail

○ **C.** AWS CloudWatch

○ **D.** AWS VPC Flow Logs

Explanation :

Answer – A
If you want to have a packet analysis tool ,then you need to an external tool. Wireshark is one such tool which will give you a detailed packet tracing.
Options B,C and D are all incorrect since these tools cannot conduct deep packet analysis.
For more information on Wireshark, please refer to the below URL

- https://www.wireshark.org/ (https://www.wireshark.org/)

Ask our Experts 👍 👎

QUESTION 8 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You’ve setup an EC2 Instance in a VPC. You are trying to ping the instance but are not able to do so. You have verified the following

a. Internet gateway attached to the VPC

b. Route tables added for the Internet gateway

c. Public IP address assigned to the Instance

You have enabled VPC flow logs and can see a rejection request for the outgoing traffic

```
2 123456789111 eni-3456b8ca 54.0.113.12 172.31.16.140 0 0 1 4 336 1432917027
1432917142 ACCEPT OK
```

```
2 123456789111 eni-3456b8ca 172.31.16.140 54.0.113.12 0 0 1 4 336 1432917094
1432917142 REJECT OK
```

What can be done to ensure that the ping request will work

○ **A.** Ensure that the NACL allows inbound ICMP request

○ **B.** Ensure that the NACL allows outbound ICMP request ✓

○ **C.** Ensure that the Security Group allows inbound ICMP request

○ **D.** Ensure that the Security Group allows outbound ICMP request

Explanation :

Answer – B
Option A is incorrect since it is the outbound traffic which is causing the issue
Options C and D are incorrect since the Security Groups are stateful and since the ICMP incoming is being accepted , it means that the outgoing for the NACL is the issue
Since the outgoing traffic is being rejected that means that the NACL outbound rules are not allowing the traffic to flow
For more information on NACL’s, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html)

Ask our Experts

QUESTION 9 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You have a VPC and EC2 Instances hosted in the subnet. You need to diagnose layer 7 traffic and see which requests are ACCEPTED and REJECTED. Which of the following would help in fulfilling this requirement?

○ **A.** Enabling CloudTrail

○ **B.** Installing IDS on each Instance

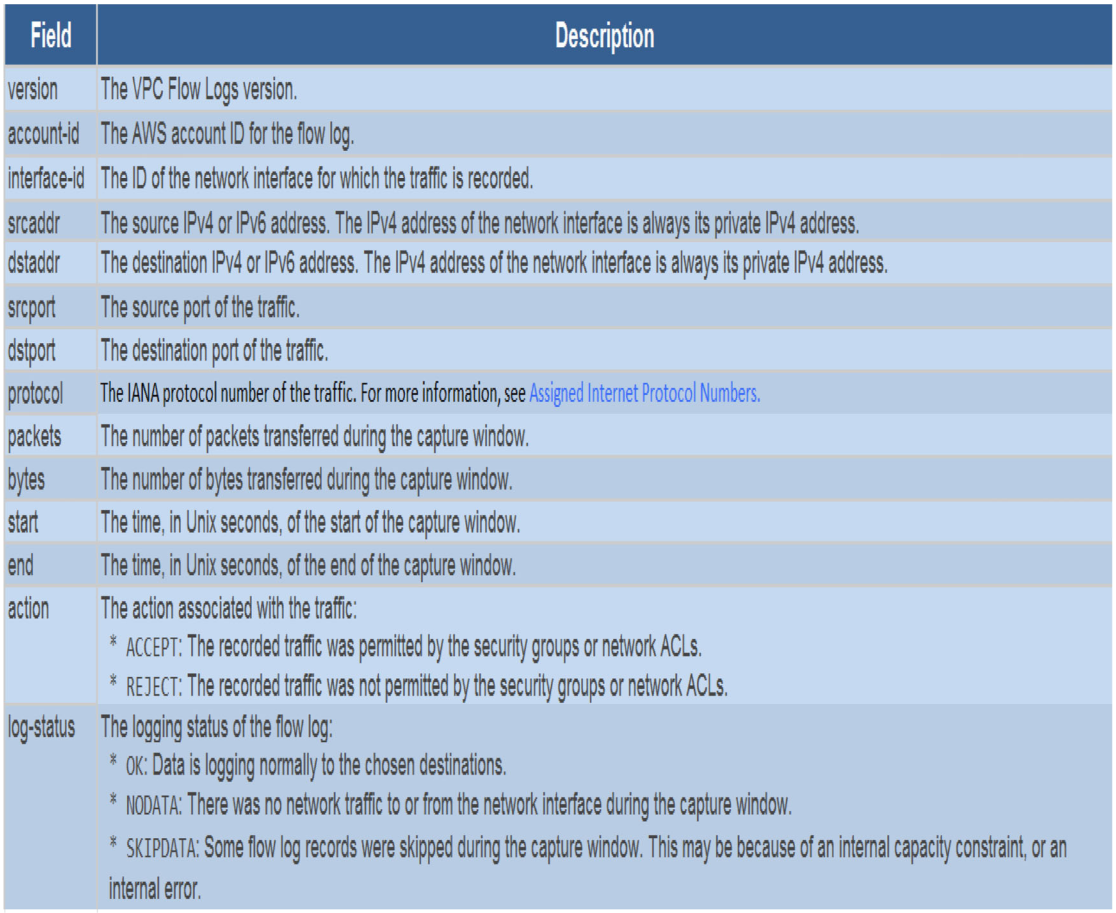
○ **C.** Enabling VPC Flow Logs ✓

○ **D.** Using Cloudwatch logs

Explanation :

Answer – C

VPC Flow logs can be used to fulfil this requirement. Below is a snippet from the AWS Documentation which shows the fields which get recorded in VPC Flow logs



Field	Description
version	The VPC Flow Logs version.
account-id	The AWS account ID for the flow log.
interface-id	The ID of the network interface for which the traffic is recorded.
srcaddr	The source IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
dstaddr	The destination IPv4 or IPv6 address. The IPv4 address of the network interface is always its private IPv4 address.
srcport	The source port of the traffic.
dstport	The destination port of the traffic.
protocol	The IANA protocol number of the traffic. For more information, see Assigned Internet Protocol Numbers.
packets	The number of packets transferred during the capture window.
bytes	The number of bytes transferred during the capture window.
start	The time, in Unix seconds, of the start of the capture window.
end	The time, in Unix seconds, of the end of the capture window.
action	The action associated with the traffic: * ACCEPT: The recorded traffic was permitted by the security groups or network ACLs. * REJECT: The recorded traffic was not permitted by the security groups or network ACLs.
log-status	The logging status of the flow log: * OK: Data is logging normally to the chosen destinations. * NODATA: There was no network traffic to or from the network interface during the capture window. * SKIPDATA: Some flow log records were skipped during the capture window. This may be because of an internal capacity constraint, or an internal error.

For more information on VPC Flow logs, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html)

Ask our Experts 👍 👎

QUESTION 10 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You have working on creating a VPN connection between AWS and your on-premise infrastructure. You've created the Virtual private gateway , and the customer gateway. You need to ensure the firewall rules are set on your side. Which of the following would you configure? Choose 2 answers from the options given below

□ **A.** TCP port 500

□ **B.** TCP port 50

□ **C.** UDP port 500 ✓

□ **D.** UDP port 50

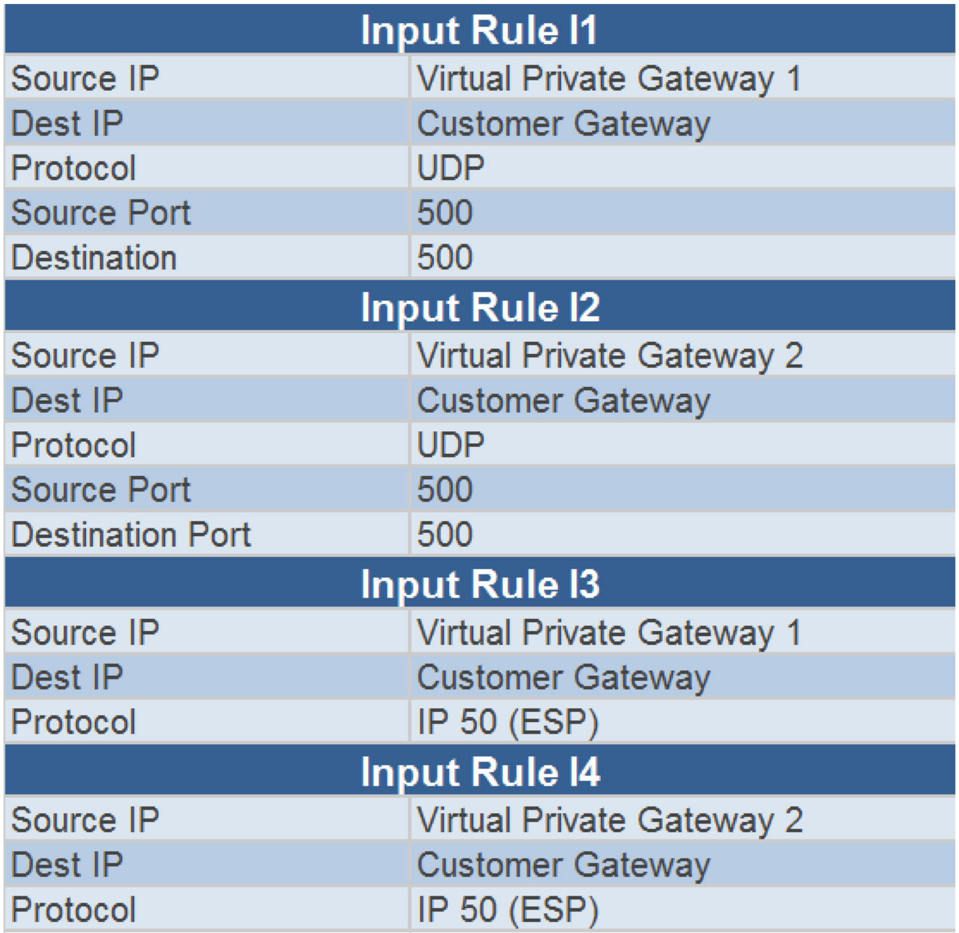
□ **E.** IP protocol 5

□ **F.** IP protocol 50 ✓

Explanation :

Answer – C and F

This is given in the AWS Documentation



Input Rule I1	
Source IP	Virtual Private Gateway 1
Dest IP	Customer Gateway
Protocol	UDP
Source Port	500
Destination	500
Input Rule I2	
Source IP	Virtual Private Gateway 2
Dest IP	Customer Gateway
Protocol	UDP
Source Port	500
Destination Port	500
Input Rule I3	
Source IP	Virtual Private Gateway 1
Dest IP	Customer Gateway
Protocol	IP 50 (ESP)
Input Rule I4	
Source IP	Virtual Private Gateway 2
Dest IP	Customer Gateway
Protocol	IP 50 (ESP)

All other options become incorrect because of the configuration mentioned in the AWS Documentation

For more information on the firewall rules, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#FirewallRules (https://docs.aws.amazon.com/AmazonVPC/latest/NetworkAdminGuide/Introduction.html#FirewallRules)

Ask our Experts 👍 👎

QUESTION 11 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You design cloudformation templates which are used to provision infrastructure for your company's account. This is the primary way in which resources can be created. But apart from Cloudformation , the company wants to get automated alerts if any other resources get created. Choose 3 services from the below list that can help accomplish this.

□ **A.** AWS Config ✓

□ **B.** AWS Lambda ✓

□ **C.** Simple Notification Service ✓

□ **D.** Cloudformation

□ **E.** Opswork

□ **F.** Cloudwatch Logs

Explanation :

Answer – A,B and C
The AWS Config service is specifically used for this purpose. Any resource changes can trigger a lambda function and notifications via the SNS service. The AWS Documentation mentions the following on the AWS config service
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations. With Config, you can review changes in configurations and relationships between AWS resources, dive into detailed resource configuration histories, and determine your overall compliance against the configurations specified in your internal guidelines. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.
Option D is invalid because Cloudformation is already used as a service in the question
Option E is invalid because this is used for creating stacks of resources like Cloudformation
Option F is invalid because this will not give a trail of what resources got created.
For more information on the AWS Config service, please refer to the below URL

- https://aws.amazon.com/config/ (https://aws.amazon.com/config/)

Ask our Experts

QUESTION 12 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have a Lambda function that is designed to probe for events on an EC2 Instance. After the probe is complete , the lambda function needs to send requests to an SQS queue. How can this be achieved? Select 2 Answers.

□ **A.** Create a NAT instance in the VPC ✓

□ **B.** Ensure that the VPC configuration is added to the Lambda function ✓

□ **C.** Ensure that the Lambda function details are added to the VPC configuration

□ **D.** Ensure that IpV6 is enabled for the subnet hosting the Lambda function

Explanation :

Answer – A and B

The AWS Documentation mentions the following to support this

AWS Lambda uses the VPC information you provide to set up ENIs that allow your Lambda function to access VPC resources. Each ENI is assigned a private IP address from the IP address range within the Subnets you specify, but is not assigned any public IP addresses. Therefore, if your Lambda function requires Internet access (for example, to access AWS services that don't have VPC endpoints), you can configure a NAT instance inside your VPC or you can use the Amazon VPC NAT gateway.

Option C is incorrect because this is not the right configuration

Option D is incorrect because this is not required for the Lambda function to work

For more information on Lambda and the VPC, please refer to the below URL

- https://docs.aws.amazon.com/lambda/latest/dg/vpc.html (https://docs.aws.amazon.com/lambda/latest/dg/vpc.html)

Ask our Experts 👍 👎

QUESTION 13 UNATTEMPTED AUTOMATE AWS TASKS

You want to automated the VPC Peering connections that occurs in your AWS Account. Which of the following methods can be used to automate the VPC peering connections.

○ **A.** Use a Cloudformation template to peer the VPC's ✓

○ **B.** Use an Opswork stack to peer the VPC's

○ **C.** Use Cloudtrail along with a Lambda function

○ **D.** Use Cloudwatch metrics along with a Lambda function

Explanation :

Answer – A

An example of this is given in the AWS Documentation

AWS::EC2::VPCPeeringConnection

A VPC peering connection enables a network connection between two virtual private clouds (VPCs) so that you can route traffic between them using a private IP address. For more information about VPC peering and its limitations, see VPC Peering Overview in the Amazon VPC Peering Guide.

Note

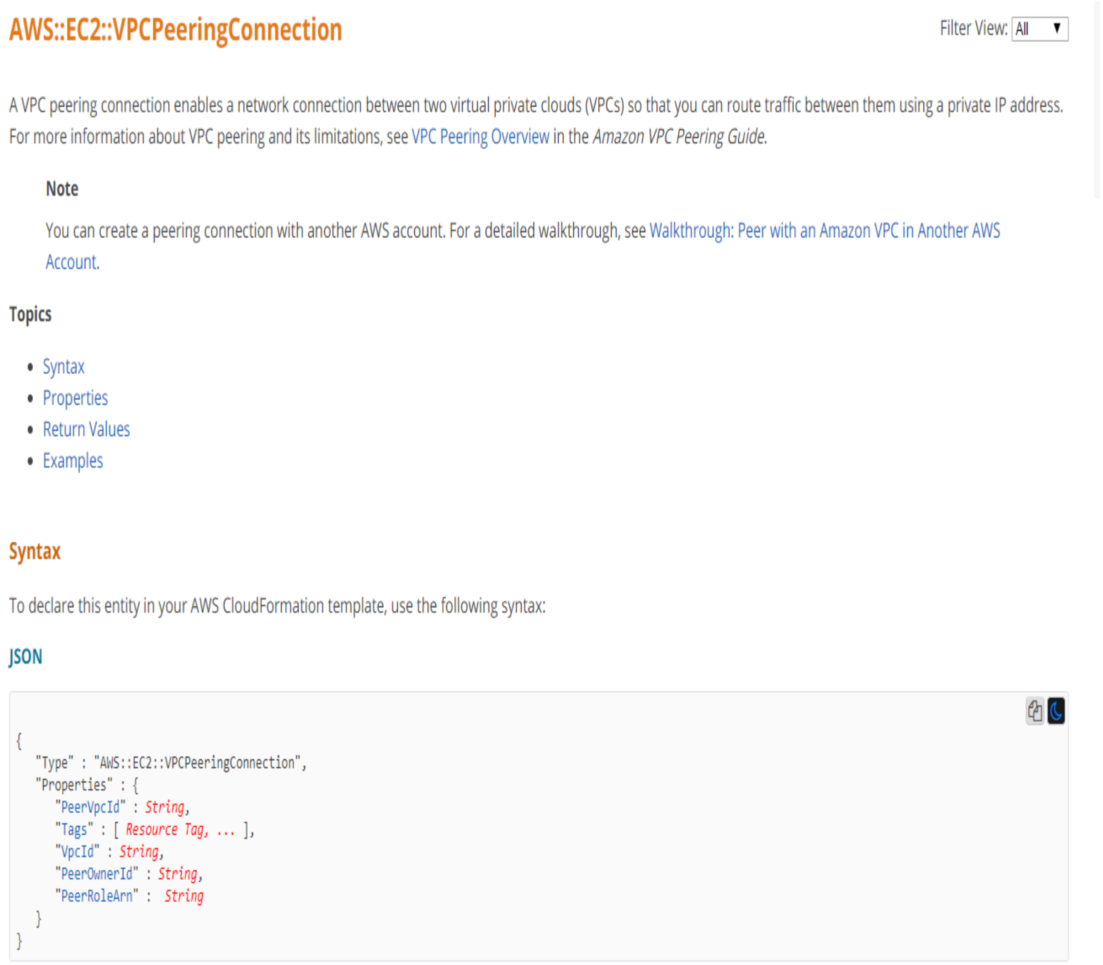
You can create a peering connection with another AWS account. For a detailed walkthrough, see Walkthrough: Peer with an Amazon VPC in Another AWS Account.

Topics

- Syntax
- Properties
- Return Values
- Examples
- Syntax

To declare this entity in your AWS CloudFormation template, use the following syntax:

JSON



AWS::EC2::VPCPeeringConnection

A VPC peering connection enables a network connection between two virtual private clouds (VPCs) so that you can route traffic between them using a private IP address. For more information about VPC peering and its limitations, see VPC Peering Overview in the *Amazon VPC Peering Guide*.

Note

You can create a peering connection with another AWS account. For a detailed walkthrough, see Walkthrough: Peer with an Amazon VPC in Another AWS Account.

Topics

- Syntax
- Properties
- Return Values
- Examples

Syntax

To declare this entity in your AWS CloudFormation template, use the following syntax:

JSON

```
{
  "Type" : "AWS::EC2::VPCPeeringConnection",
  "Properties" : {
    "PeerVpcId" : String,
    "Tags" : [ Resource Tag, ... ],
    "VpcId" : String,
    "PeerOwnerId" : String,
    "PeerRoleArn" :  String
  }
}
```

Option B is incorrect since Cloudformation should be used instead of Cloudformation
Options C and D are incorrect since these would not assist in the automatic creation of resources
For more information on VPC peering with Cloudformation, please refer to the below URL

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpcpeeringconnection.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-resource-ec2-vpcpeeringconnection.html)

Ask our Experts 👍 👎

QUESTION 14 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have an EC2 Instance which will be responsible for processing a lot of video and audio. There is a requirement to ensure that the EC2 Instance has the maximum performance when it comes to the network packet processing. How can this be achieved? Choose 2 answers from the options given below

□ **A.** Ensure that the instance supports single root I/O virtualization ✓

□ **B.** Ensure that the MTU is set to 9001 on the Instance ✓

□ **C.** Ensure that the MTU is set to 9001 for the VPC

□ **D.** Choose a t2.medium instance type

Explanation :

Answer – A and B
The AWS Documentation mentions the following
Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies.
Also when it comes to setting the MTU , you can enable Jumbo frames by setting the MTU to 9001
Option C is incorrect since the MTU needs to be set on the Instance
Option D is incorrect since this instance type will not support Enhanced Networking
For more information on Enhanced Networking, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html)

Ask our Experts 👍 👎

QUESTION 15 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have a set of EC2 instances in a VPC located at US-East-1. You need to have optimal network performance on these instances. These instances will talk to instances in another VPC located at US-East-2 via VPC Peering. Which of the following should be carried out to ensure maximum network performance? Choose 2 answers from the options given below.

☐ **A.** Enable Enhanced Networking on the Instances ✓

☐ **B.** Set the MTU on the Instances to 9001

☐ **C.** Ensure the operating system supports Enhanced networking ✓

☐ **D.** Create 2 availability zones for the instances in the primary VPC and place them in aplacement group

Explanation :

Answer – A and C

Option B is incorrect since the MTU of 9001 will not work in VPC peering. The maximum that is allowable in VPC peering is 1500

For placement groups to work , the instances must be placed in the same availability zone.

The AWS Documentation mentions the following

Enhanced networking uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities on supported instance types. SR-IOV is a method of device virtualization that provides higher I/O performance and lower CPU utilization when compared to traditional virtualized network interfaces. Enhanced networking provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies.

For more information on Enhanced Networking, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html)

When we implement intraregion VPC peering jumbo frames provide MTU of 9001 provided both the instances does support Jumbo frames.

When we implement inter region VPC Peering the maximum MTU that we receive with Jumbo frames is 1500.

Ask our Experts

QUESTION 16 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You have an EC2 Instance that will act as a custom origin for a Cloudfront web distribution. You need to ensure that traffic is encrypted completely in transit. Which of the following step is part of the process to achieve this.

○ **A.** Configure the Viewer protocol policy as Redirect HTTP to HTTPS and Change the Origin Protocol policy to Match Viewer ✓

○ **B.** Configure the Viewer protocol policy as HTTP and ensure that SSL certificate is installed on the EC2 Instance

○ **C.** Configure the Viewer protocol policy as HTTPS and ensure that the traffic flows via the Amazon Virtual Private Network

○ **D.** Configure the Viewer protocol policy as Redirect HTTP to HTTPS and ensure that the traffic flows via the Amazon Virtual Private Network

Explanation :

Answer – A

The AWS Documentation clearly mentions the configuration for the Distribution in such a scenario

Origin Protocol Policy

Change the Origin Protocol Policy for the applicable origins in your distribution:

- HTTPS Only – CloudFront uses only HTTPS to communicate with your custom origin.
- Match Viewer – CloudFront communicates with your custom origin using HTTP or HTTPS, depending on the protocol of the viewer request. For example, if you choose Match Viewer for Origin Protocol Policy and the viewer uses HTTPS to request an object from CloudFront, CloudFront also uses HTTPS to forward the request to your origin.
- Choose Match Viewer only if you specify Redirect HTTP to HTTPS or HTTPS Only for Viewer Protocol Policy.
- CloudFront caches the object only once even if viewers make requests using both HTTP and HTTPS protocols.

Origin SSL Protocols

Choose the Origin SSL Protocols for the applicable origins in your distribution. The SSLv3 protocol is less secure, so we recommend that you choose SSLv3 only if your origin doesn't support TLSv1 or later.

Note

The TLSv1 handshake is both backwards and forwards compatible with SSLv3, but TLSv1.1 and TLSv1.2 are not. In this case, the openssl only sends a SSLv3 handshake.

Option B is incorrect since the Viewer Protocol should not be HTTP

Options C and D are incorrect since you cannot specify the traffic to flow in Cloudfront through a Amazon Virtual Private Network
For more information on using HTTPS for a custom origin, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/using-https-cloudfront-to-custom-origin.html)

Ask our Experts

QUESTION 17 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You need to create a Private VIF for an existing AWS Direct Connect connection. Which of the following is required during the configuration process? Please select the 2 correct options from below.

☐ **A.** The Peer Public IP

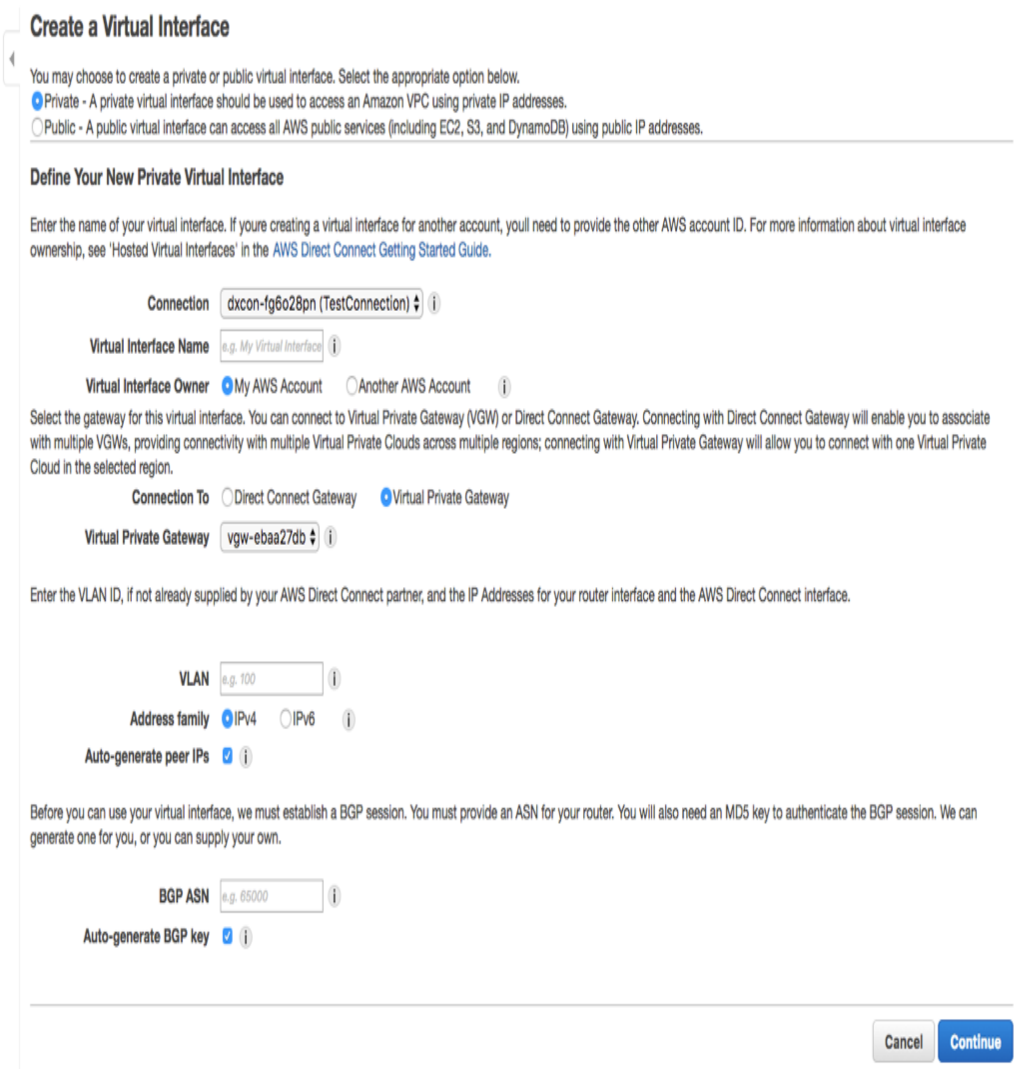
☐ **B.** VLAN ID ✓

☐ **C.** Virtual Gateway ✓

☐ **D.** Prefixes to advertise

Explanation :

Answer – B and C
If you look at the screen for creating a private VIF, this is how it looks like. Here you can see that VLAN ID and the Virtual Private gateway is part of the creation process



Create a Virtual Interface

You may choose to create a private or public virtual interface. Select the appropriate option below.

● Private - A private virtual interface should be used to access an Amazon VPC using private IP addresses.

○ Public - A public virtual interface can access all AWS public services (including EC2, S3, and DynamoDB) using public IP addresses.

Define Your New Private Virtual Interface

Enter the name of your virtual interface. If youre creating a virtual interface for another account, youll need to provide the other AWS account ID. For more information about virtual interface ownership, see 'Hosted Virtual Interfaces' in the AWS Direct Connect Getting Started Guide.

Connection: dxcon-fg6o28pn (TestConnection)

Virtual Interface Name: e.g. My Virtual Interface

Virtual Interface Owner: ● My AWS Account ○ Another AWS Account

Select the gateway for this virtual interface. You can connect to Virtual Private Gateway (VGW) or Direct Connect Gateway. Connecting with Direct Connect Gateway will enable you to associate with multiple VGWs, providing connectivity with multiple Virtual Private Clouds across multiple regions; connecting with Virtual Private Gateway will allow you to connect with one Virtual Private Cloud in the selected region.

Connection To: ○ Direct Connect Gateway ● Virtual Private Gateway

Virtual Private Gateway: vgw-ebaa27db

Enter the VLAN ID, if not already supplied by your AWS Direct Connect partner, and the IP Addresses for your router interface and the AWS Direct Connect interface.

VLAN: e.g. 100

Address family: ● IPv4 ○ IPv6

Auto-generate peer IPs: ☑

Before you can use your virtual interface, we must establish a BGP session. You must provide an ASN for your router. You will also need an MD5 key to authenticate the BGP session. We can generate one for you, or you can supply your own.

BGP ASN: e.g. 65000

Auto-generate BGP key: ☑

Options A and D are incorrect since this is required when creating a public VIF

For more information on the creation of Virtual Interfaces, please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/create-vif.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

A company has setup a set of EC2 Instances behind an Application Load Balancer. There seems to be a barrage of requests from a series of URL's. You need to have these URL's blacklisted. How can you achieve this on an ongoing manner?

○ **A.** Deny the URL’s via the Security Groups for the Instance

○ **B.** Deny the URL’s via the NACL’s for the subnet

○ **C.** Put a WAF in front of the Application Load Balancer ✔

○ **D.** Use AWS VPC Flow logs to prevent the attacks from the URL’s

Explanation :

Answer – C
Options A and B are incorrect since these can be used to blacklist IP’s
Option D is incorrect since this cannot be used prevent attacks from the Internet
The AWS Documentation mentions the following
AWS WAF is a web application firewall that helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block to your web applications by defining customizable web security rules. You can use AWS WAF to create custom rules that block common attack patterns, such as SQL injection or cross-site scripting, and rules that are designed for your specific application. New rules can be deployed within minutes, letting you respond quickly to changing traffic patterns. Also, AWS WAF includes a full-featured API that you can use to automate the creation, deployment, and maintenance of web security rules.
For more information on the AWS WAF, please refer to the below URL

- https://aws.amazon.com/waf/ (https://aws.amazon.com/waf/)

Ask our Experts 👍 👎

QUESTION 19 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are trying to diagnose a connection issue with a Linux instance. The instance is assigned a public IP and is in the public subnet. You can also see that the Internet gateway is attached and the route tables are in place. You SSH into the instance from a bastion host. You then do an ifconfig and see that the interface does not have a public IP address. What should be done next to check the issue

○ **A.** Assign the public IP to the Interface

○ **B.** Assign an Elastic IP to the interface

○ **C.** Check the Security Groups for the instance ✔

○ **D.** Assign a private IP to the interface

Explanation :

Answer – C
You need to check the security groups to see if the instance is accepting traffic from the internet. One might be directed to think that the issue is because the ifconfig does not have a public IP address. The following from the AWS Documentation should be taken into consideration
The public IPv4 address is displayed as a property of the network interface in the console, but it's mapped to the primary private IPv4 address through NAT. Therefore, if you inspect the properties of your network interface on your instance, for example, through ifconfig (Linux) or ipconfig (Windows), the public IPv4 address is not displayed. To determine your instance's public IPv4 address from within the instance, you can use instance metadata
In such a scenario all other options become invalid
For more information on using Instance addressing, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-instance-addressing.html)

Ask our Experts

QUESTION 20 UNATTEMPTED
CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Which one of the following is not true about Amazon CloudFront cache behaviors ?

○ **A.** For RTMP distributions, you can configure CloudFront to forward query string parameters to your origin. ✓

○ **B.** Forward query strings to the origin, and cache based on all parameters in the query string.

○ **C.** Forward query strings to the origin, and cache based on specified parameters in the query string.

○ **D.** Don't forward query strings to the origin at all then CloudFront doesn't cache based on query string parameters.

Explanation :

Answer – A
For RTMP distributions, you cannot configure CloudFront to forward query string parameters to your origin.
Options B,C and D are true.

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/QueryStringParameters.html)

Ask our Experts

QUESTION 21 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

A company has setup an application on an EC2 Instance in a private subnet. This Instance is used to process videos. The Instance has been enabled with Enhanced Networking. The Instance now needs to get videos from an S3 bucket for processing. An IAM Role has been assigned to the Instance to access S3. But when the EC2 Instance tries to access the S3 bucket , a 403 error is returned. What needs to be done to ensure that the error gets resolved?

○ **A.** Ensure that VPC endpoint is created and associate it with subnets via route tables created inside selected VPC ✓

○ **B.** Ensure that a VPC endpoint is created and attached to the EC2 Instance

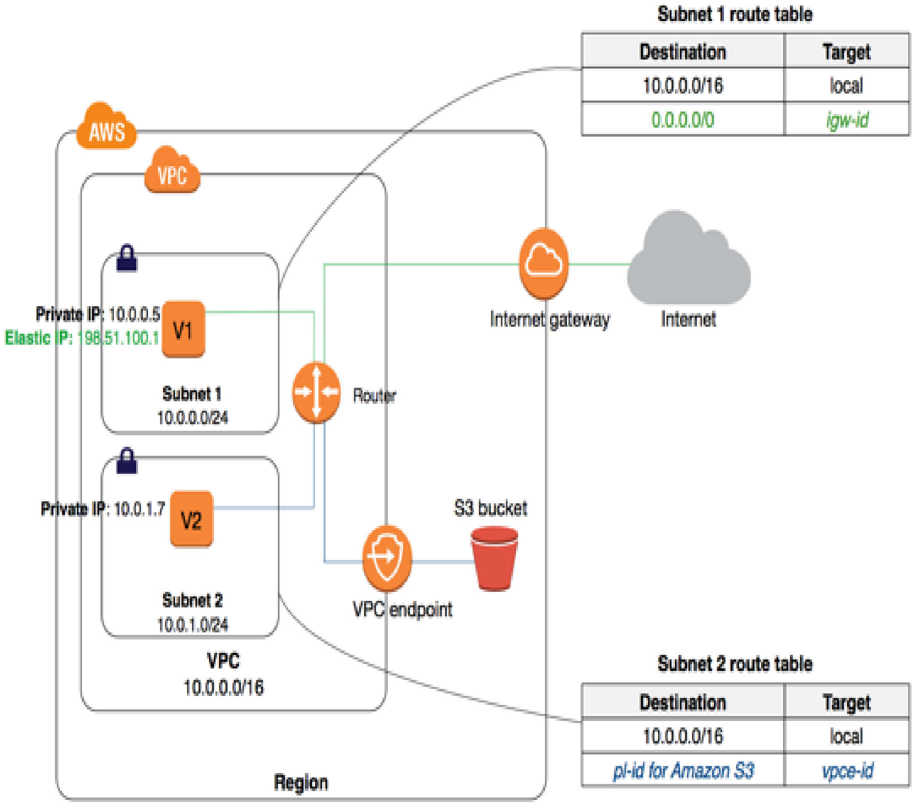
○ **C.** Ensure that the CIDR range for the S3 bucket is added to the Security Groups for theEC2 Instance

○ **D.** Ensure that the CIDR range for the S3 bucket is added to the NACL's for the subnet

Explanation :

Answer – A

You need to setup a gateway endpoint for this. The below architecture diagram shows how this can be setup



Subnet 1 route table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	*igw-id*

Subnet 2 route table

Destination	Target
10.0.0.0/16	local
pl-id for Amazon S3	*vpce-id*

Option B is incorrect since the VPC endpoint needs to be associated with the EC2 Instance

Options C and D are incorrect since adding the CIDR range will not help

For more information on VPC gateways, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpce-gateway.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpce-gateway.html)

Ask our Experts

QUESTION 22 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You work for your company as an AWS administrator. You've setup a Classic Load balancer and EC2 Instances for an application. You have setup HTTPS listeners with the default security policies. Your Security department has mentioned that the security policy defined for the load balancer does not meet the regulations defined for the policy. What changes would you make to be in line with the requirements of the IT security department.

○ **A.** Create a new SSL and associate it with the underlying EC2 Instances

○ **B.** Create a new SSL and associate it with the underlying Classic Load balancer

○ **C.** Create a custom security policy and associate it with the EC2 Instance

○ **D.** Create a custom security policy and associate it with the Classic Load Balancer ✓

Explanation :

Answer – D
You can create a custom Security policy which is in line with the IT security department and then associate it with the Classic Load Balancer.
Options A and B are incorrect since you don't need to change the SSL certificates
Option C is incorrect since you need to change the security policy with the ELB
For more information on Security Policies for the Classic Load Balancer, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-config-update.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ssl-config-update.html)

Ask our Experts 👍 👎

QUESTION 23 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on delivering content via an application hosted on a set of EC2 Instances. The end devices can be laptops , mobile devices , tablets etc. The content needs to be customized based on the type of end user device. Which of the following can help fulfil this requirement and also ensure that cost is MINIMIZED and MAXIMUM ease of deployment?

Select 2 answers.

□ **A.** Application Load Balancers ✓

□ **B.** Cloudfront with Lambda@Edge ✓

□ **C.** Network Load Balancers

□ **D.** Appstream 2.0

Explanation :

Answer – A and B
Option C is incorrect since this is the wrong type of Load Balancer to use for this purpose
Option D is incorrect since AppStream is the incorrect service to use for this requirement.
The Application Load balancers can be used to distribute the processing powers to different Instances based on the type of request
The AWS Documentation mentions the following about Lambda@Edge which supports the requirement
CloudFront can return different objects to viewers based on the device they're using by checking the User-Agent header, which includes information about the devices. For example, CloudFront can return different images based on the screen size of their device.
For more information on Lambda@Edge, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/lambda-at-the-edge.html)

Ask our Experts 👍 👎

QUESTION 24 UNATTEMPTED
CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company has a 3 tier application that consists of a Web , Application and Database Tier. The application is based on delivering RESTful services. They have Autoscaling Groups for the EC2 Instances for the Web and Application Tier. You now want to add high availability to the Tiers, but it needs to ensured that each tier can be scaled independently. How would you architect. Choose the most PREFERRED option.

○ **A.** Create an Application Load Balancer and add separate target groups for the Web and Application Tier. ✓

○ **B.** Create an Application Load Balancer for the Application Tier and a classic load balancer for the Web Tier

○ **C.** Create a Classic Load Balancer and add multiple targets for the Web and Application Tier.

○ **D.** Create separate Classic Load Balancers for the Web and Application Tiers.

Explanation :

Answer – A

An Application Load Balancer functions at the application layer, the seventh layer of the Open Systems Interconnection (OSI) model. After the load balancer receives a request, it evaluates the listener rules in priority order to determine which rule to apply, and then selects a target from the target group for the rule action. You can configure listener rules to route requests to different target groups based on the content of the application traffic.

Application Load Balancer supports a round-robin load-balancing algorithm. Additionally, Application Load Balancer supports a slow start mode with the round-robin algorithm that allows you to add new targets without overwhelming them with a flood of requests. With the slow start mode, targets warm up before accepting their fair share of requests based on a ramp-up period that you specify. Slow start is very useful for applications that depend on cache and need a warm-up period before being able to respond to requests with optimal performance.

It does support HTTP/HTTPS protocols. Compared with Classic Load Balancers an Application Load Balancer does provides more features such as host based routing, slow start etc which is ideal for web and application traffic load balancing.
The AWS Documentation also mentions independent working of target groups under the Application Load Balancer
Support for monitoring the health of each service independently, as health checks are defined at the target group level and many CloudWatch metrics are reported at the target group level. Attaching a target group to an Auto Scaling group enables you to scale each service dynamically based on demand.
For more information on the Application Load Balancer, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html)

Ask our Experts 👍 👎

QUESTION 25 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You've setup an a Classic Load Balancer and EC2 Instances behind the Load Balancer. The following Security Groups have been set

- Security Group for the ELB – Accept Incoming traffic on port 80 from 0.0.0.0/0

- Security Group for the EC2 Instances – Accept Incoming traffic on port 80 from 0.0.0.0/0

It has been noticed that the EC2 Instances are getting a large number of direct requests from the Internet. What should be done to resolve the issue.

○ **A.** Change the ELB security group to only accept traffic from the EC2 Instances on port 80

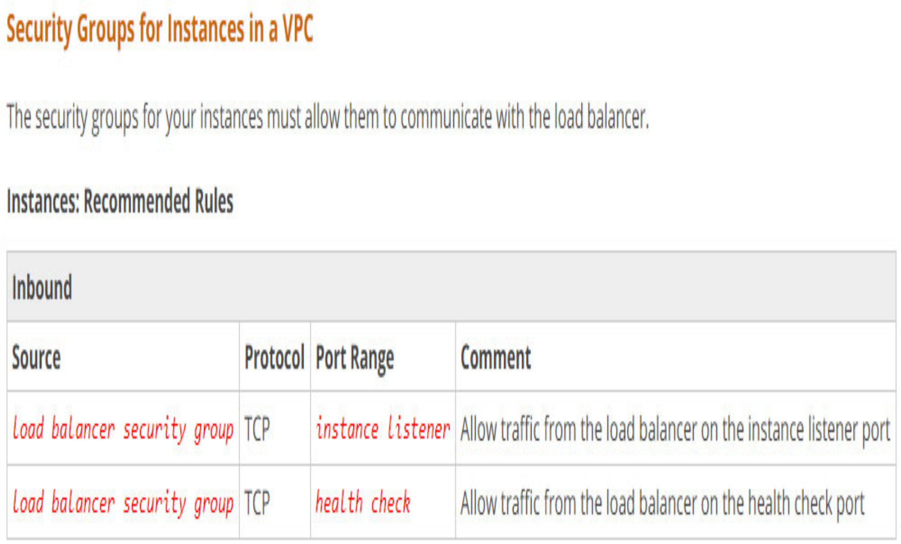
○ **B.** Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 80 ✔

○ **C.** Change the ELB security group to only accept traffic from the EC2 Instances on port443

○ **D.** Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 443

Explanation :

Answer – B
The AWS Documentation mentions the following for how the security groups should be defined for the underlying EC2 Instances



Security Groups for Instances in a VPC

The security groups for your instances must allow them to communicate with the load balancer.

Instances: Recommended Rules

Inbound			
Source	Protocol	Port Range	Comment
load balancer security group	TCP	*instance listener*	Allow traffic from the load balancer on the instance listener port
load balancer security group	TCP	*health check*	Allow traffic from the load balancer on the health check port

Option A is incorrect since the ELB needs to accept traffic from everywhere.

Options C and D are incorrect since there is no mention in the question on HTTPS traffic
For more information on the Security Groups for Classic Load Balancers, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-security-groups.html)

Ask our Experts

QUESTION 26 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

When creating an AWS workspace , which of the following is required for the creation of the workspace.

○ **A.** A VPC with a private and public subnet

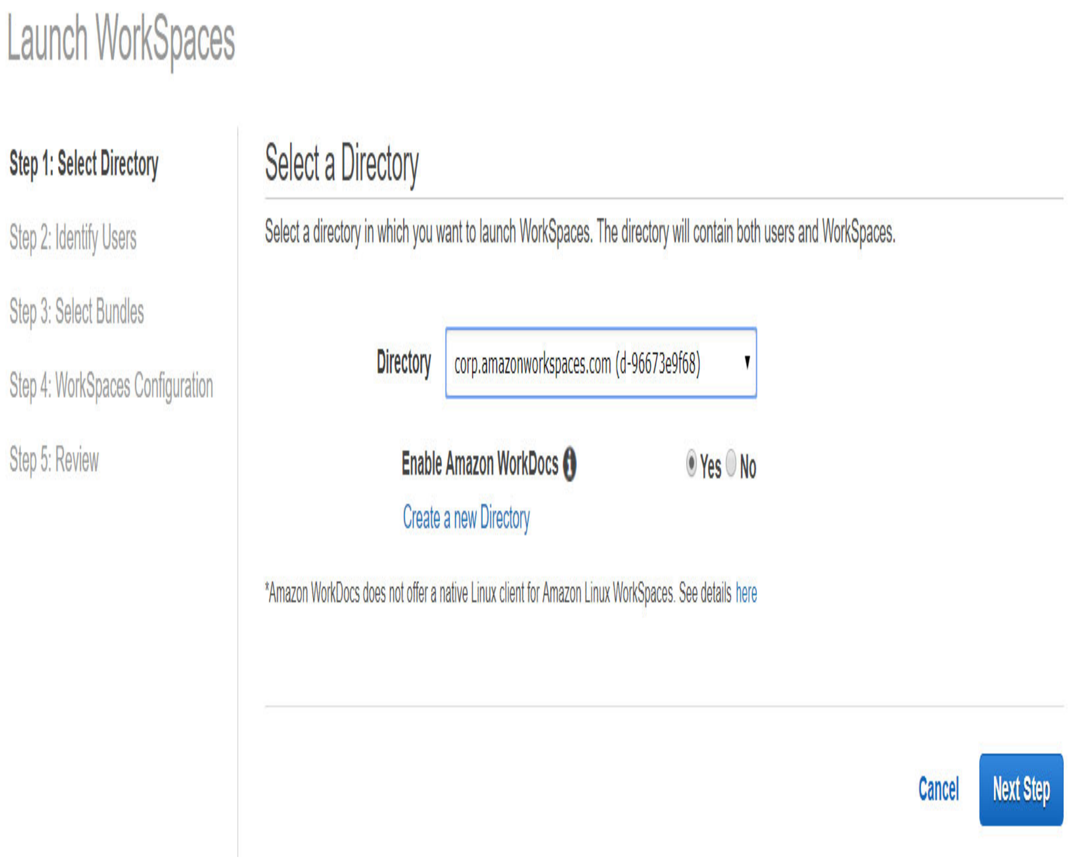
○ **B.** A User directory ✓

○ **C.** A NAT instance on the customer side

○ **D.** An AWS Direct Connect connection

Explanation :

Answer – B
When you create a workspace as shown below , you need to choose an existing User Directory



Launch WorkSpaces

Step 1: Select Directory

Step 2: Identify Users

Step 3: Select Bundles

Step 4: WorkSpaces Configuration

Step 5: Review

Select a Directory

Select a directory in which you want to launch WorkSpaces. The directory will contain both users and WorkSpaces.

Directory: corp.amazonworkspaces.com (d-96673e9f68)

Enable Amazon WorkDocs: ● Yes ○ No

Create a new Directory

*Amazon WorkDocs does not offer a native Linux client for Amazon Linux WorkSpaces. See details here

All other options are invalid , since the minimum requirement is shown in the screen above

For more information on AWS workspaces, please refer to the below URL

- https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html (https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have created an Application Load Balancer. You need to point your domain names of www.example.com and example.com to the Application Load Balancer. Your Hosted zone is example.com. How can you achieve this?

○ **A.** Create one CNAME record for the ELB to www.example.com.And then create another CNAME record to the ELB to example.com

○ **B.** Create an Alias record for example.com and point it to the ELB as the target. Create a CNAME record for www.example.com and point it to example.com ✓

○ **C.** Create an ALIAS record for the ELB and point it to example.com. Create a PTR record for www.example.com and point it toexample.com

○ **D.** Create one CNAME record for the ELB to www.example.com.And then create another PTR record to the ELB to example.com

Explanation :

Answer – B

The AWS Documentation mentions below on ALIAS records which can be created

Choosing Between Alias and Non-Alias Records

Amazon Route 53 alias records provide a Route 53–specific extension to DNS functionality. Alias records let you route traffic to selected AWS resources, such as CloudFront distributions and Amazon S3 bucket. They also let you route traffic from one record in a hosted zone to another record.

Unlike a CNAME record, you can create an alias record at the top node of a DNS namespace, also known as the zone apex. For example, if you register the DNS name example.com, the zone apex is example.com. You can't create a CNAME record for example.com, but you can create an alias record for example.com that routes traffic to www.example.com.

When Route 53 receives a DNS query for an alias record, Route 53 responds with the applicable value for that resource:

- A CloudFront distribution – Route 53 responds with one or more IP addresses for CloudFront edge servers that can serve your content.

- An Elastic Beanstalk environment – Route 53 responds with one or more IP addresses for the environment.
- An ELB load balancer – Route 53 responds with one or more IP addresses for the load balancer.
- An Amazon S3 bucket that is configured as a static website – Route 53 responds with one IP address for the Amazon S3 bucket.
- Another Route 53 record in the same hosted zone – Route 53 responds as if the query is for the record that is referenced by the alias record.

You can then create a CNAME record for www.example.com.
Option A is incorrect because you cannot create a CNAME record at the zone apex
Options C and D are incorrect since PTR records cannot be used.
For more information on alias and non-alias records, please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resource-record-sets-choosing-alias-non-alias.html)

Ask our Experts 👍 👎

QUESTION 28 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You need to setup a Cross Connect with AWS Direct Connect. You already have the necessary equipment in place. You now need to complete the connection process. How can you achieve this?

○ **A.** Contact your provider ✓

○ **B.** Raise a support ticket with AWS

○ **C.** Raise a AWS Direct Connect request in the AWS Console

○ **D.** Contact an AWS Partner

Explanation :

Answer – A
This is mentioned in the AWS Documentation
After you have downloaded your Letter of Authorization and Connecting Facility Assignment (LOA-CFA), you need to complete your cross-network connection, also known as a *cross connect*. If you already have equipment located in an AWS Direct Connect location, contact the appropriate provider

to complete the cross connect. For specific instructions for each provider, see the table below. Contact your provider for cross connect pricing. After the cross connect is established, you can create the virtual interfaces using the AWS Direct Connect console.

Because of this , all other options are automatically invalid.

For more information on Cross connect, please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Colocation.html)

Ask our Experts 👍 👎

QUESTION 29 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company is planning on setting up an AWS Direct Connect connection along with a private VIF. The company has 169 IP prefixes that will be advertised via the private VIF. The company has raised the request and ensured that the equipment is in place. What is an implementation step that they need to consider to ensure the connection works as desired?

○ **A.** Ensure to also create a public VIF to access the resources in the VPC.

○ **B.** Summarise the routes into a default route ✔

○ **C.** Create a VPN connection

○ **D.** Ensure a VPC Peering connection is in place

Explanation :

Answer – B

When troubleshooting AWS Direct Connect , one of the key issues is to ensure that the number of IP Prefixes summarised is below 100. Hence one of the steps would be to ensure that the routes are summarised into a default route.

Option A is incorrect since you don't need a public VIF to access the resources in a VPC

Options C and D are incorrect since there is no mention in the question for any other sort of connection requirements.

For more information on Troubleshooting AWS Direct Connect Issues, please refer to the below URL

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html)

Ask our Experts 👍 👎

QUESTION 30 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

There is a requirement to see all port scans which are occurring on a couple of EC2 instances. Which of the following can be used for such a requirement?

○ **A.** AWS Inspector

○ **B.** AWS Trusted Advisor

○ **C.** AWS VPC Flow Logs ✓

○ **D.** AWS Cloudwatch Events

Explanation :

Answer – C
The AWS Documentation mentions the following
VPC Flow Logs is a feature that enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. After you've created a flow log, you can view and retrieve its data in Amazon CloudWatch Logs.
So you can use VPC Flow logs to see if certain ports are being accessed frequently.
Option A is incorrect since this can only check for vulnerabilities in systems
Options B and D are incorrect since these tools cannot be used for port scans
For more information on VPC Flow Logs, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html)

Ask our Experts 👍 👎

QUESTION 31 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have created a VPC Endpoint for your private subnet to S3. The default endpoint policy is in place. You are trying to access a bucket , but you're getting an access denied error. What must be done.

○ **A.** Add the VPC endpoint to the Endpoint policy to allow access to the S3 bucket

○ **B.** Add the VPC to the S3 bucket policy

○ **C.** Add the VPC Endpoint to the S3 bucket policy ✓

○ **D.** Add the VPC endpoint to the Bucket ACL

Explanation :

Answer – C
Option A is incorrect since the default endpoint policy already will allow complete S3 access
Option B is incorrect since the right approach is to add the VPC Endpoint to the S3 bucket policy
Option D is incorrect since you are not supposed to add this to the Bucket ACL.
You need to ensure that the S3 bucket allows access to the VPC Endpoint. Below is a sample from the AWS Documentation.
Restricting Access to a Specific VPC Endpoint

The following is an example of an S3 bucket policy that restricts access to a specific bucket, examplebucket, only from the VPC endpoint with the ID vpce-1a2b3c4d. The policy denies all access to the bucket if the specified endpoint is not being used. The aws:sourceVpce condition is used to the specify the endpoint. The aws:sourceVpce condition does not require an ARN for the VPC endpoint resource, only the VPC endpoint ID. For more information about using conditions in a policy, see Specifying Conditions in a Policy.

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
   {
    "Sid": "Access-to-specific-VPCE-only",
    "Principal": "*",
    "Action": "s3:*",
    "Effect": "Deny",
    "Resource": ["arn:aws:s3:::examplebucket",
          "arn:aws:s3:::examplebucket/*"],
    "Condition": {
     "StringNotEquals": {
      "aws:sourceVpce": "vpce-1a2b3c4d"
     }
    }
   }
  ]
}
```

For more information on VPC endpoints and S3 bucket policies, please refer to the below URL

- https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html (https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies-vpc-endpoint.html)

Ask our Experts 👍 👎

QUESTION 32 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company currently hosts an application that consists of a NGINX web server that is hosted behind a load balancer. You need to ensure that you restrict access to certain locations for the content hosted on the Web server. How can you accomplish this?

○ **A.** Use the NGINX logs to get the web server variable and then use the IP address to restrict content via Cloudfront geo-restrictions.

○ **B.** Use the ELB logs to create a blacklist for restrictions.

○ **C.** Use the IP addresses in the X-Forwarded-For HTTP header and then restrict content via Cloudfront geo-restrictions. ✓

○ **D.** Use the ELB itself to restrict content via geo-restrictions.

Explanation :

Answer – C

Such use case scenarios are given in the AWS Documentation

Task list for restricting access to files in a CloudFront distribution based on geographic location

1. Get an account with a geolocation service.
2. Upload your content to an Amazon Simple Storage Service (S3) bucket. For more information, see the Amazon S3 documentation.
3. Configure Amazon CloudFront and Amazon S3 to serve private content. For more information, see Serving Private Content with Signed URLs and Signed Cookies.
4. Write your web application to do the following:

- Send the IP address for each user request to the geolocation service.
- Evaluate the return value from the geolocation service to determine whether the user is in a location to which you want CloudFront to distribute your content.
- Based on whether you want to distribute your content to the user's location, either generate a signed URL for your CloudFront content, or return HTTP status code 403 (Forbidden) to the user. Alternatively, you can configure CloudFront to return a custom error message. For more information, see Creating a Custom Error Page for Specific HTTP Status Codes.

For more information, refer to the documentation for the geolocation service that you're using.
You can use a web server variable to get the IP addresses of the users who are visiting your website. Note the following caveats:

- If your web server is not connected to the internet through a load balancer, you can use a web server variable to get the remote IP address. However, this IP address isn't always the user's IP address—it can also be the IP address of a proxy server, depending on how the user is connected to the internet.
- If your web server is connected to the internet through a load balancer, a web server variable might contain the IP address of the load balancer, not the IP address of the user. In this configuration, we recommend that you use the last IP address in the X-Forwarded-For http header. This header typically contains more than one IP address, most of which are for proxies or load balancers. The last IP address in the list is the one most likely to be associated with the user's geographic location.

If your web server is not connected to a load balancer, we recommend that you use web server variables instead of the X-Forwarded-For header to avoid IP address spoofing.

Option A is invalid since the web server variable could have the IP of the proxy server
Options B and D are invalid since the ELB would not be able to provide geo level restrictions
For more information on restricting access via Cloudfront, please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html)

Ask our Experts 👍 👎

QUESTION 33 UNATTEMPTED
CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your planning on setting up a VPC with Subnets. The EC2 Instances hosted in the VPC needs to get the time from a custom NTP server. How can you accomplish this?

○ **A.** Create a DHCP Options set and provide the NTP server name ✔

○ **B.** Define a resource record in Route 53 and provide the NTP server name

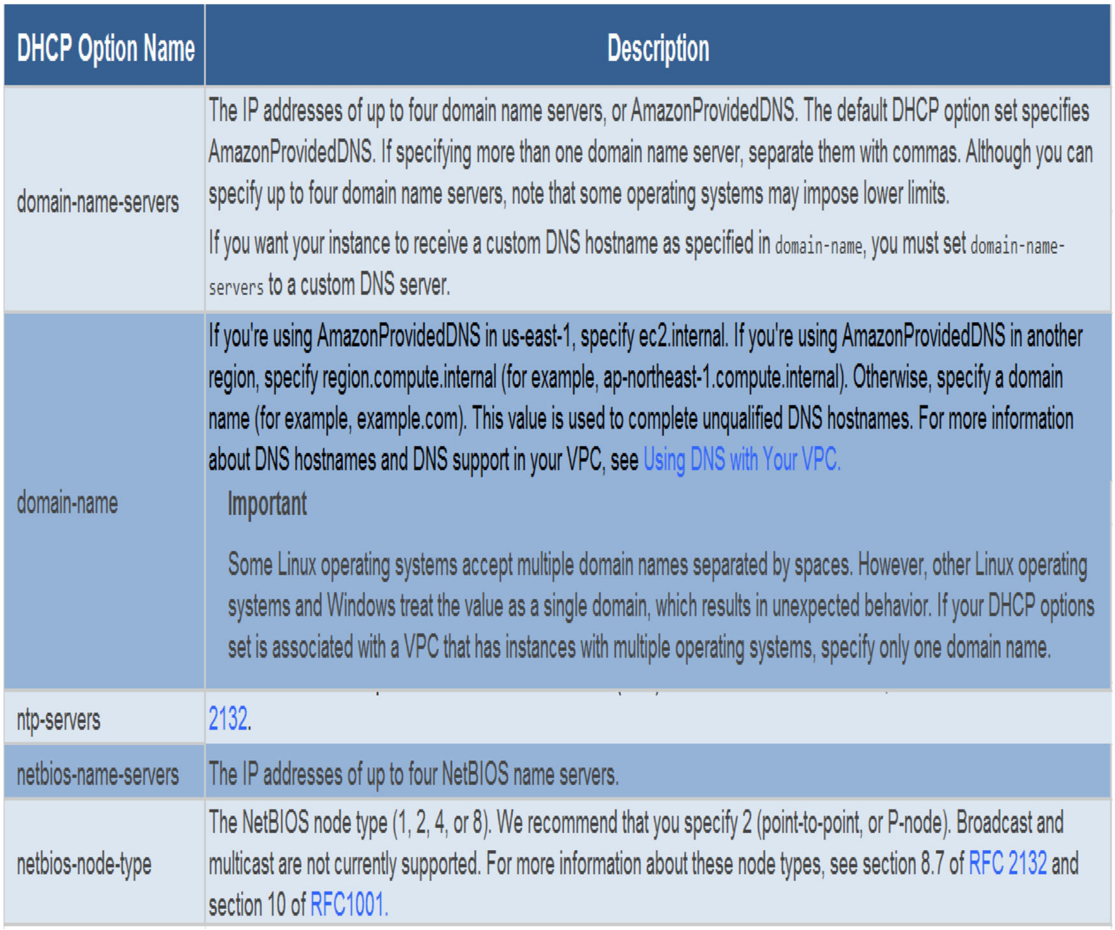
○ **C.** Assign the NTP server in the Subnet configuration

○ **D.** Use an Application Load Balancer and then provide the NTP server as part of the ALB configuration.

Explanation :

Answer – A

You can create a new DHCP options set and then provide the NTP server name as part of the options set. Below is from the AWS Documentation which shows the configuration possible in the DHCP options set.



DHCP Option Name	Description
domain-name-servers	The IP addresses of up to four domain name servers, or AmazonProvidedDNS. The default DHCP option set specifies AmazonProvidedDNS. If specifying more than one domain name server, separate them with commas. Although you can specify up to four domain name servers, note that some operating systems may impose lower limits. If you want your instance to receive a custom DNS hostname as specified in `domain-name`, you must set `domain-name-servers` to a custom DNS server.
domain-name	If you're using AmazonProvidedDNS in us-east-1, specify ec2.internal. If you're using AmazonProvidedDNS in another region, specify region.compute.internal (for example, ap-northeast-1.compute.internal). Otherwise, specify a domain name (for example, example.com). This value is used to complete unqualified DNS hostnames. For more information about DNS hostnames and DNS support in your VPC, see Using DNS with Your VPC. Important Some Linux operating systems accept multiple domain names separated by spaces. However, other Linux operating systems and Windows treat the value as a single domain, which results in unexpected behavior. If your DHCP options set is associated with a VPC that has instances with multiple operating systems, specify only one domain name.
ntp-servers	2132.
netbios-name-servers	The IP addresses of up to four NetBIOS name servers.
netbios-node-type	The NetBIOS node type (1, 2, 4, or 8). We recommend that you specify 2 (point-to-point, or P-node). Broadcast and multicast are not currently supported. For more information about these node types, see section 8.7 of RFC 2132 and section 10 of RFC1001.

All other options are invalid as the configurations mentioned are invalid

For more information on the DHCP Options Set, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_DHCP_Options.html)

Ask our Experts

QUESTION 34 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company has setup a Classic Load Balancer with EC2 Instances behind them. These EC2 Instances are spun up via an Autoscaling group. In your company there is normally a spike in traffic in the beginning and end of the day. The ELB and

Autoscaling Groups have been created with the default settings. It has been noticed that there are timeouts or partially rendered pages at times. How can this be resolved?

○ **A.** Change the maximum number of Instances setting in the Auto scaling Group

○ **B.** Change the Connection Draining timeout in the ELB ✓

○ **C.** Enable Cross Zone Load Balancing

○ **D.** Add another Autoscaling group to the ELB

Explanation :

Answer – B
The most likely reason is that when the instances are getting terminated by Autoscaling, the requests are being partially fulfilled and not completed. In such as case you can increase the connection draining on the ELB.
Option A is invalid because it is when the Instances are terminating that is the issue
Option C is invalid because this will only balance the requests
Option D is invalid because you don't need multiple Autoscaling groups for this
For more information on Connection Draining, please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/config-conn-drain.html)

Ask our Experts 👍 👎

QUESTION 35 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has many VPC's , one for Development , one for Staging , one for Production and one Management VPC. It is required for traffic to flow from the other VPC's to the Management VPC's. The VPC's should also be traversable via the on-premise infrastructure. How would you architect the solution with the least amount of effort?

○ **A.** Creating a VPC peering connection between the VPC's. Create a VPN connection between the Management VPC and the on-premise environment.

○ **B.** Creating a VPC peering connection between the VPC's. Create a VPN connection between all the VPC's and the on-premise environment. ✓

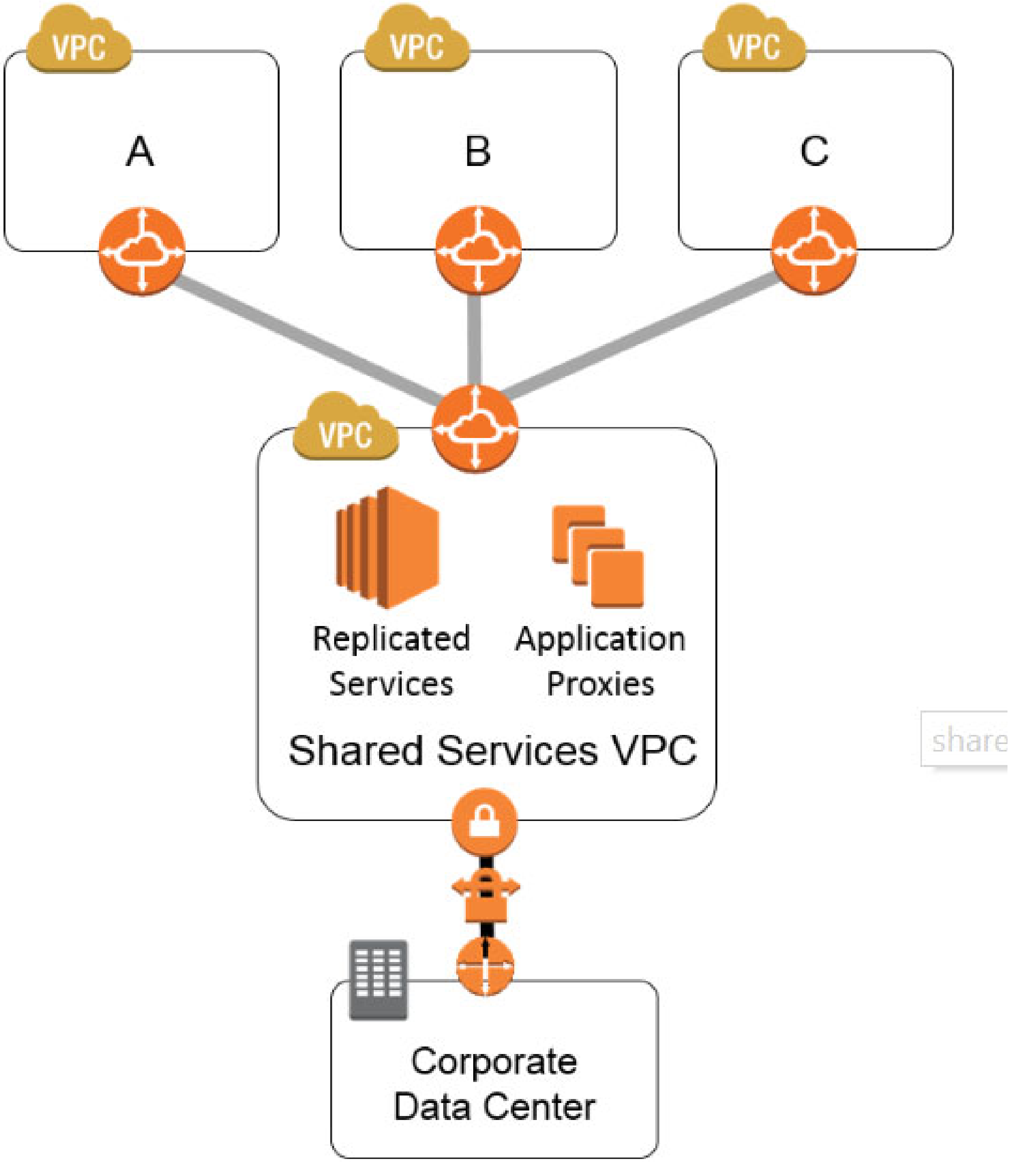
○ **C.** Create a Virtual Private gateway connection between all of the VPC's. Create a VPN connection between the Management VPC and the on-premise environment.

○ **D.** Create a VPN connection between the Management VPC and all other VPC's. Create a VPNconnection between the Management VPC and the on-premise environment.

Explanation :

Answer – B

This is an example of a shared services VPC. The below snippet from the AWS Documentation shows the architecture around this.



Option A is incorrect because the on-premise resources cannot traverse the other VPC's via the Peering connection

Option C is incorrect because of the incorrect use of the Virtual Private gateway
Option D is incorrect because of the overall maintenance for the activities being performed.
For more information on VPC and VPN connection sharing , please refer to the below URL

- https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/ (https://aws.amazon.com/answers/networking/aws-multiple-vpc-vpn-connection-sharing/)

Ask our Experts

QUESTION 36 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has created an AWS Direct Connect connection. A virtual private gateway is attached to a VPC. Around 111 routes are being advertised on from On-premise. A private VIF is being created to the VPGW. But the Virtual Interface is always showing as down. What needs to be done to ensure the interface comes back up.

○ **A.** Ensure that a VPN connection is also in place for the tunnel to become active.

○ **B.** Ensure less routes are being advertised. ✓

○ **C.** Ensure that static routes are put in place

○ **D.** Ensure that the IP sec configuration is correct

Explanation :

Answer – B
The main issue is that more than 100 routes are being advertised , hence the tunnel is not coming up.
All other options are incorrect because all of these refer to VPN connections
For more information on troubleshooting AWS Direct Connect connections , please refer to the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html)

Ask our Experts

QUESTION 37 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You’ve setup a private hosted zone in Route 53. You’ve setup a VPN connection between the AWS VPC and your on-premise network. You need to ensure that you can resolve DNS names from on-premise to the resources records defined in the Private hosted zone. How can you accomplish this?

○ **A.** Create a DNS resolver server in your on-premise location. Configure the VPC with a new DHCP options set which uses this DNS resolver.

○ **B.** Create a DNS forwarder server in your on-premise location. Configure the VPC with anew DHCP options set which uses this DNS forwarder.

○ **C.** Configure a DNS forwarder in the VPC which will forward DNS requests to the Route 53 private hosted zone ✓

○ **D.** Configure a DNS resolver in the VPC which will resolve DNS requests to the Route 53 private hosted zone

Explanation :

Answer – C

Options A and D are incorrect since you need to use a DNS forwarder

Option B is incorrect since the forwarder needs to be defined in the VPC.

Such an example is also given in the AWS Documentation

Issue

How can I resolve Amazon Route 53 private hosted zones from an on-premises network via an Ubuntu instance?

Resolution

You can resolve domain names in private hosted zones from your on-premises network by configuring a DNS forwarder. The following instructions assume that your on-premises network is configured with a VPN or AWS Direct Connect to an AWS VPC, and a Route 53 private hosted zone is associated with that VPC.

For full details on this configuration, please refer to the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/r53-private-ubuntu/ (https://aws.amazon.com/premiumsupport/knowledge-center/r53-private-ubuntu/)

Ask our Experts 👍 👎

QUESTION 38 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company has the requirement of connecting their on-premise location to an AWS VPC. The On-premise servers should have the capabilities of resolving custom DNS domain names in the VPC. The Instances in the VPC need to have the ability to resolve the DNS names of the on-premise servers. How can you achieve this?

○ **A.** Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Amazon DNS resolver for the VPC. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location. ✔

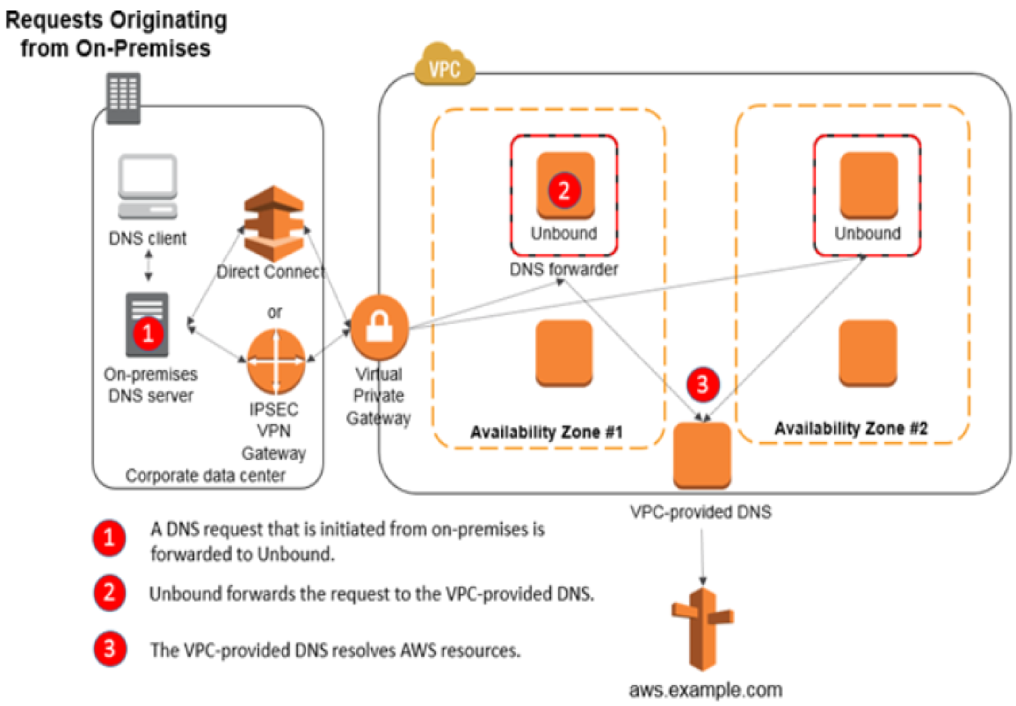
○ **B.** Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Name server for the Route 53 hosted zone. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

○ **C.** Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the On-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

○ **D.** Setup DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the VPN tunnel. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

Explanation :

Answer – A
Option B is incorrect because the DNS forwarder needs to point to the DNS resolver for the VPC and not the Name servers.
Option C is incorrect because the DNS forwarder should also point to the DNS resolver for the VPC
Option D is incorrect because the DNS forwarder should not point to the VPN tunnel IP address.
An example of this is given in the AWS Documentation



1 A DNS request that is initiated from on-premises is forwarded to Unbound.

2 Unbound forwards the request to the VPC-provided DNS.

3 The VPC-provided DNS resolves AWS resources.

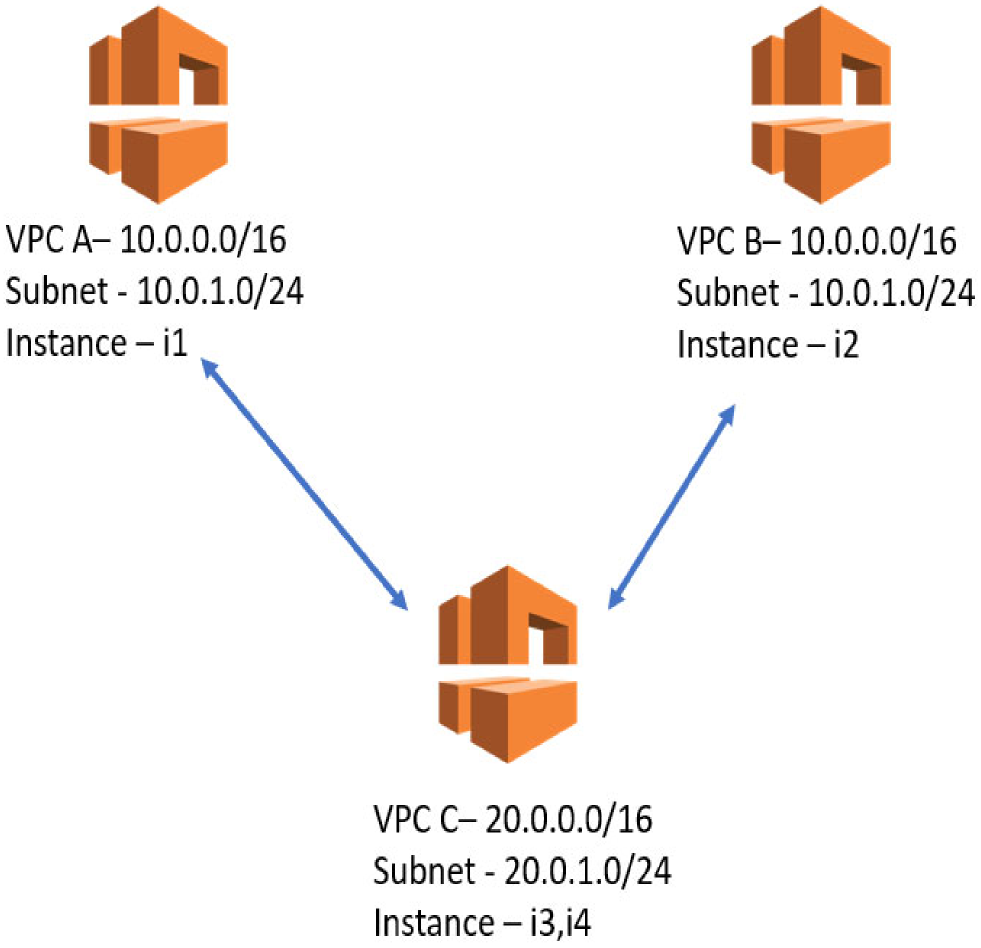
For more information on this example , please refer to the below URL

- https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-by-using-unbound/ (https://aws.amazon.com/blogs/security/how-to-set-up-dns-resolution-between-on-premises-networks-and-aws-by-using-unbound/)

Ask our Experts

QUESTION 39 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You are trying to implement the below architecture



So you have a VPC peering connection between VPC A and VPC C and another one between VPC B and VPC C.

You have Instances defined in each subnet as shown above. You need to ensure the following

- Instance i3 can communicate with Instance i1 but not Instance i2
- Instance i4 can communicate with Instance i2 but not Instance i1

What needs to be done so that this can accomplished. Choose 2 answers from the options given below.

□ **A.** Create 2 subnets in VPC C , ensure i3 and i4 are in different subnets ✓

□ **B.** Ensure different route tables are created to restrict access and added to the 2 different subnets ✓

□ **C.** Ensure that i3 and i4 are created in the same subnet

□ **D.** Ensure that one route table is created which restricts access and added to the subnet

Explanation :

Answer – A and B
Since VPC A and VPC B have overlapping CIDR's it will be difficult to restrict traffic if you have only one subnet. Hence create two subnets with 2 different route tables will help meet the requirement.
Options C and D are incorrect since having one subnet will not help meet the requirement.
For more information on VPC peering , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-peering.html)

Ask our Experts 👍 👎

QUESTION 40 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You have established a VPN connection between your on-premise and an AWS VPC. You need to also ensure that instances in the VPC can reach the Internet so you have also attached an Internet gateway. How would you setup the route tables to ensure traffic can flow via the VPN and the Internet.

○ **A.** Setup 2 Route tables. One route table with a default route to the Internet and another one with the default route to the Virtual Private gateway. Attach the Route tables to the subnets in the VPC.

○ **B.** Setup one route table. Add one route of 0.0.0.0/0 to the Internet and one specific prefix route for the Virtual Private gateway. Attach the Route table to the subnets in the VPC. ✓

○ **C.** Setup one route table. Add one route of 0.0.0.0/0 to the Internet and another route of 0.0.0.0/0 route for the Virtual Private gateway. Attach the Route table to the subnets in the VPC.

○ **D.** Setup 2 Route tables. One route table with a default route to the Internet andan other one with the specific prefix route to the Virtual Private gateway.Attach the Route tables to the subnets in the VPC.

Explanation :

Answer – B
You should create a specific route for the Virtual Private gateway
The AWS Documentation mentions the following
You can use an AWS managed VPN connection to enable instances in your VPC to communicate with your own network. To do this, create and attach a virtual private gateway to your VPC, and then add a route with the destination of your network and a target of the virtual private gateway (vgw-xxxxxxxx).
You can then create and configure your VPN connection
Options A and D are invalid because you can only have one route table for a subnet.
Option C is invalid since you need to have a more specific route for the Virtual Private gateway
For more information on Route tables , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html)

Ask our Experts 👍 👎

QUESTION 41 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are planning on setting up an AWS VPN managed connection. You have a customer gateway that is behind a NAT device. In such a case what steps should be taken to ensure proper connectivity. Choose 2 answers from the options given below.

□ **A.** Use the public IP address of the NAT device ✓

□ **B.** Use the private IP address of the customer gateway

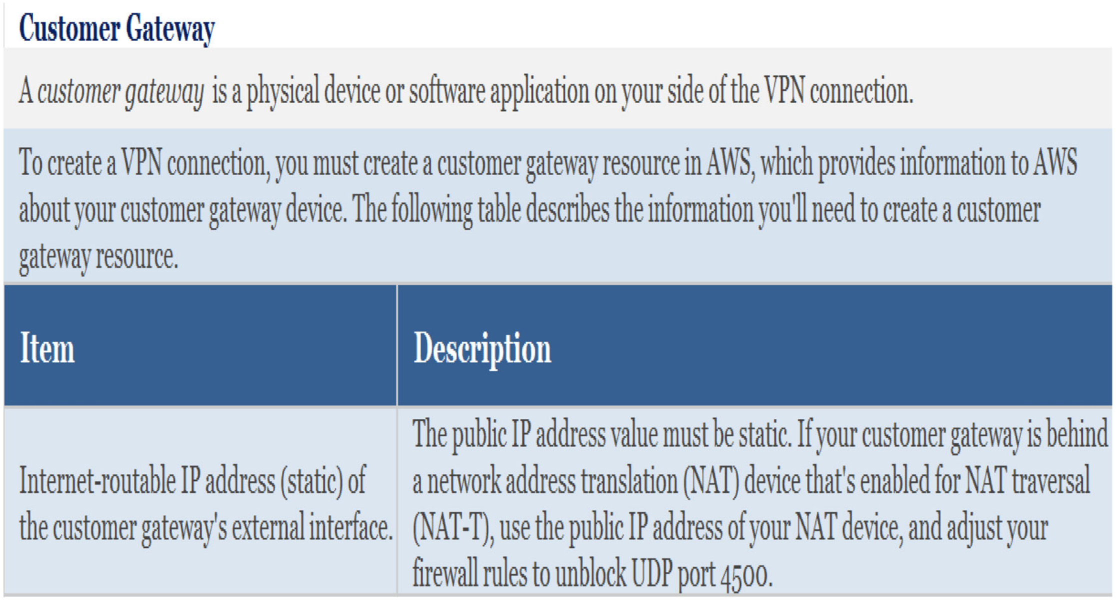
□ **C.** Ensure the on-premise firewall has UDP port 4500 unblocked ✓

□ **D.** Ensure the on-premise firewall has TCP port 4500 unblocked

Explanation :

Answer – A and C
Options B and D are incorrect since you need to mention the public IP address and also ensure that UDP port 4500 is unblocked.

This is given in the AWS Documentation



Customer Gateway

A *customer gateway* is a physical device or software application on your side of the VPN connection.

To create a VPN connection, you must create a customer gateway resource in AWS, which provides information to AWS about your customer gateway device. The following table describes the information you'll need to create a customer gateway resource.

Item	Description
Internet-routable IP address (static) of the customer gateway's external interface.	The public IP address value must be static. If your customer gateway is behind a network address translation (NAT) device that's enabled for NAT traversal (NAT-T), use the public IP address of your NAT device, and adjust your firewall rules to unblock UDP port 4500.

For more information on VPN Connections , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts 👍 👎

QUESTION 42 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has many remote branch offices that need to connect with your AWS VPC. Which of the following can help achieve this connectivity in an easy manner?

○ **A.** VPN Cloudhub ✓

○ **B.** AWS Direct Connect with a Public VIF

○ **C.** AWS Direct Connect with a Private VIF

○ **D.** VPC Peering

Explanation :

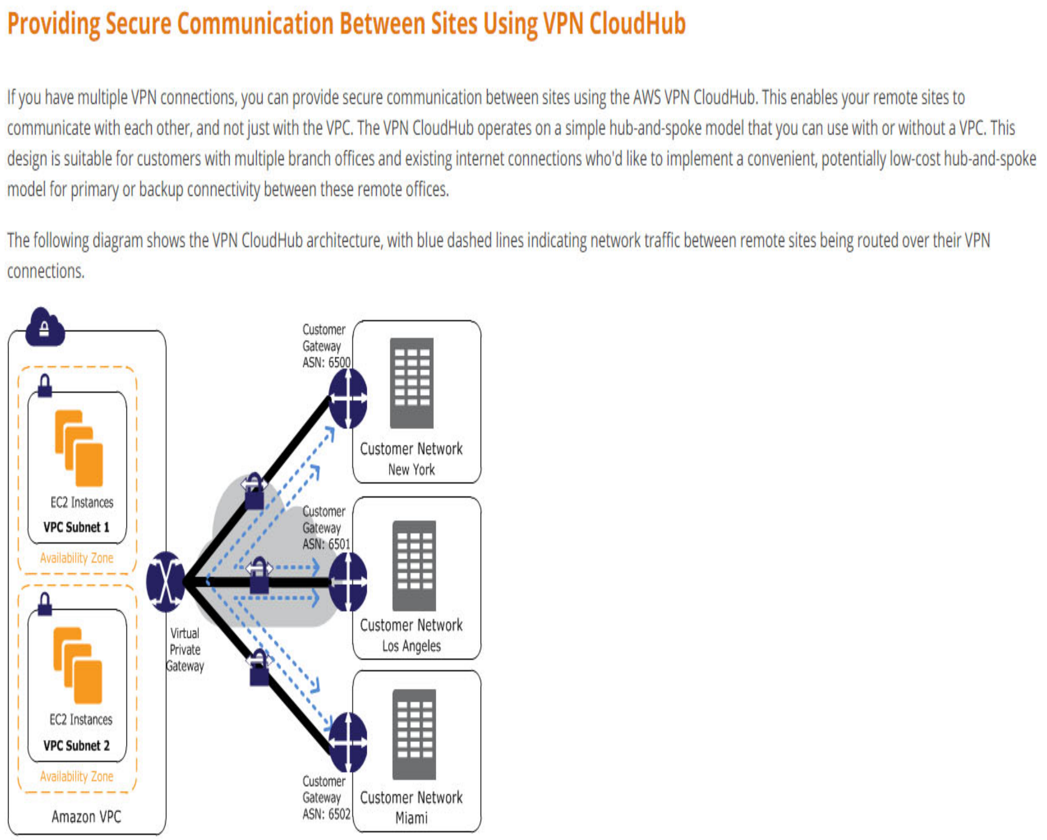
Answer – A

The AWS Documentation mentions the following

Providing Secure Communication Between Sites Using VPN CloudHub

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

The following diagram shows the VPN CloudHub architecture, with blue dashed lines indicating network traffic between remote sites being routed over their VPN connections.



Providing Secure Communication Between Sites Using VPN CloudHub

If you have multiple VPN connections, you can provide secure communication between sites using the AWS VPN CloudHub. This enables your remote sites to communicate with each other, and not just with the VPC. The VPN CloudHub operates on a simple hub-and-spoke model that you can use with or without a VPC. This design is suitable for customers with multiple branch offices and existing internet connections who'd like to implement a convenient, potentially low-cost hub-and-spoke model for primary or backup connectivity between these remote offices.

The following diagram shows the VPN CloudHub architecture, with blue dashed lines indicating network traffic between remote sites being routed over their VPN connections.

Options B and C are incorrect since this is not ideal for Remote branch offices

Option D is incorrect since this should be used to connect 2 VPC's

For more information on VPN CLoudhub , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPN_CloudHub.html)

Ask our Experts

QUESTION 43 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company needs VPN connectivity to an AWS VPC. There are around 100 mobile devices , 40 remote computers and a site office which needs to connect. How would you achieve this connectivity? Choose 2 answers from the options given below

□ **A.** Use AWS Managed VPN for the site office ✓

□ **B.** Use AWS Managed VPN for the mobile and remote computers

□ **C.** Use a custom VPN server to accept connections from the mobile and remote computers ✓

□ **D.** Use AWS Direct Connect with a public VIF for the site office

Explanation :

Answer – A and C
For the Site office , you can use the standard AWS Managed VPN
Since there is no mechanism currently for point to site connectivity for individual devices , you need to use a custom VPN server
Option B is incorrect since you cannot use AWS Managed VPN for these devices
Option D is incorrect since AWS Direct connect should not be used for this requirement
For more information on VPN Connections , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html)

Ask our Experts 👍 👎

QUESTION 44 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company needs to establish a VPN between AWS and their on-premise infrastructure. They have the following requirements

Support for RSA 4096-bit (https://www.softether.org/1-features/3._Security_and_Reliability) encryptions.
RADIUS / NT Domain user authentication function
Deep-inspect packet logging function
What can be done to achieve this requirement?

○ **A.** Use an AWS Managed VPN

○ **B.** Use a VPN from the AWS marketplace ✓

○ **C.** Use AWS Direct Connect with a Private VIF

○ **D.** Use AWS Direct Connect with a Public VIF

Explanation :

Answer - B
Since the requirements are very specific you will need to use a custom VPN from the AWS Marketplace
Hence all other options become invalid because of the very specific requirements
An example of a VPN server from the AWS Marketplace is given below

- https://aws.amazon.com/marketplace/pp/B00MI40CAE/ref=mkt_wir_openvpn_byol (https://aws.amazon.com/marketplace/pp/B00MI40CAE/ref=mkt_wir_openvpn_byol)

Ask our Experts

QUESTION 45 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have configured a hosted zone in Route 53. You need to have the ability to see the types of records being requested to the zone. How can you configure this?

○ **A.** Configure VPC Flow Logs

○ **B.** Configure Amazon Route 53 logging ✓

○ **C.** Configure Cloudwatch metrics

○ **D.** Configure Cloudtrail

Explanation :

Answer – B
This is given in the AWS Documentation
You can configure Amazon Route 53 to log information about the queries that Route 53 receives, such as the following:

- The domain or subdomain that was requested
- The date and time of the request
- The DNS record type (such as A or AAAA)
- The Route 53 edge location that responded to the DNS query
- The DNS response code, such as NoError or ServFail

Option A is invalid since this will only give the results of the requests to the VPC

Option C is invalid since this will only give metric details
Option D is invalid since this will only give API level call activity.
For more information on querying logs in Route 53 , please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/query-logs.html)

Ask our Experts

QUESTION 46 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are planning on creating a VPC endpoint for your SaaS product hosted in AWS. You will provide this link to a customer who will access the link from their application. The application works on the UDP protocol. You plan on providing the DNS name for the link to them. But the customer is not able to use the link from within their application. What could be the issue.

○ **A.** The gateway endpoint has a policy that denies access. This should be modified accordingly.

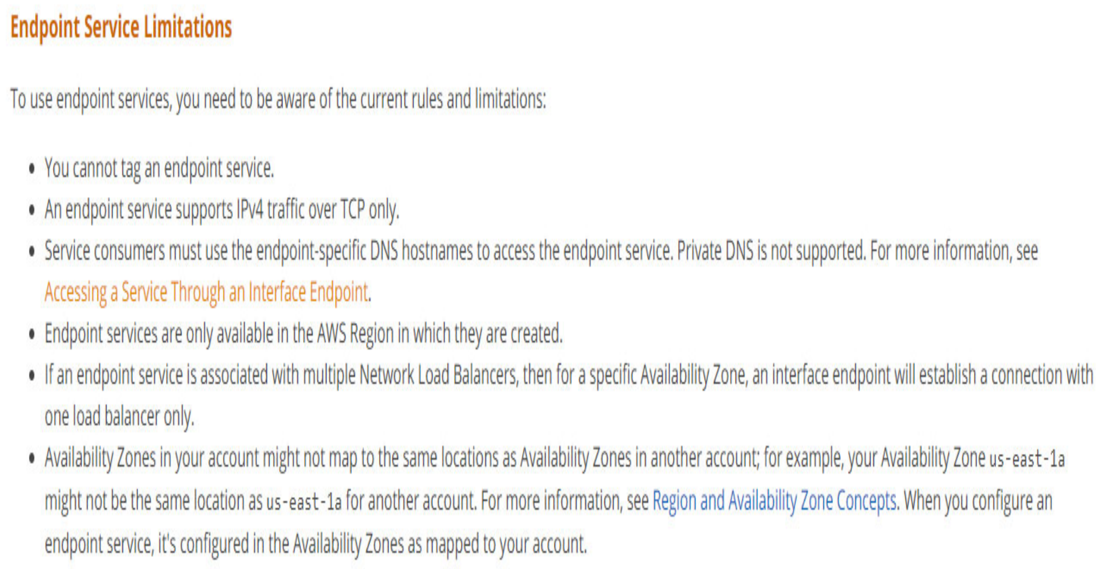
○ **B.** The service endpoint only works on the TCP protocol ✓

○ **C.** The customer needs to create a Network load balancer to access the endpoint service

○ **D.** The customer needs to use a NAT device to access the endpoint service

Explanation :

Answer – B
This is mentioned as one of the limitations for Endpoint Services in the AWS Documentation



Endpoint Service Limitations

To use endpoint services, you need to be aware of the current rules and limitations:

- You cannot tag an endpoint service.
- An endpoint service supports IPv4 traffic over TCP only.
- Service consumers must use the endpoint-specific DNS hostnames to access the endpoint service. Private DNS is not supported. For more information, see Accessing a Service Through an Interface Endpoint.
- Endpoint services are only available in the AWS Region in which they are created.
- If an endpoint service is associated with multiple Network Load Balancers, then for a specific Availability Zone, an interface endpoint will establish a connection with one load balancer only.
- Availability Zones in your account might not map to the same locations as Availability Zones in another account; for example, your Availability Zone `us-east-1a` might not be the same location as `us-east-1a` for another account. For more information, see Region and Availability Zone Concepts. When you configure an endpoint service, it's configured in the Availability Zones as mapped to your account.

Option A is incorrect since this is an interface and not a gateway

Options C and D are incorrect since you don't need a NAT device or Network Load Balancer to access the service
For more information on Service Endpoints , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/endpoint-service.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/endpoint-service.html)

Ask our Experts 👍 👎

QUESTION 47 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company needs to create its own VPN based EC2 Instances. These Instances will allow 2 VPC's in different regions to talk to each other. You've created one VPN instance in one subnet in one VPC and another Instance in another subnet in another VPC. You are establishing the communication via Internet gateway. What extra consideration should be in place in such a configuration.

○ **A.** Placing a NAT instance in front of both of the VPN connections

○ **B.** Placing a Virtual private gateway as the termination endpoint

○ **C.** Using a Private hosted zone in Route 53

○ **D.** Having multiple VPN Instances for high availability ✓

Explanation :

Answer - D

You have to consider the high availability of the Instances. In AWS Managed VPN , there are 2 tunnels created , so automatically there is high availability in place. But here if either Instance goes down the connection is broken.

Options A and C are incorrect since these are not key requirements

Option B is incorrect since the individual EC2 Instances are the termination points

For more information on such an example , please visit the below link

- https://aws.amazon.com/articles/connecting-multiple-vpcs-with-ec2-instances-ipsec/ (https://aws.amazon.com/articles/connecting-multiple-vpcs-with-ec2-instances-ipsec/)

Ask our Experts 👍 👎

QUESTION 48 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You need to have a managed threat detection service that continuously monitors for malicious or unauthorized behaviour against your EC2 Instances. Which of the following can help in such a requirement?

○ **A.** Amazon GuardDuty ✓

○ **B.** Amazon CloudTrail

○ **C.** Amazon VPC Flow Logs

○ **D.** Amazon Cloudwatch Logs

Explanation :

Answer – A

The AWS Documentation mentions the following

Amazon GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. It monitors for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. GuardDuty also detects potentially compromised instances or reconnaissance by attackers.

Option B is incorrect since this is used for API Monitoring

Option C is incorrect since this is used for monitoring traffic in the VPC

Option D is incorrect since this is used for logging purposes

For more information on Amazon GuardDuty , please visit the below link

- https://aws.amazon.com/guardduty/ (https://aws.amazon.com/guardduty/)

Ask our Experts 👍 👎

QUESTION 49 UNATTEMPTED AUTOMATE AWS TASKS

You are creating a Cloudformation template that will used to automate the provisioning of VPC's and Subnets. You need to allow for dynamic provisioning aspects as to which Availability zone , the subnet needs to be created. Which part of the template would help in provisioning such dynamic values

○ **A.** Parameters ✓

○ **B.** Output

○ **C.** Tags

○ **D.** Change Sets

Explanation :

Answer – A

This is also provided in the AWS Documentation

Parameters

"Use the optional Parameters section to customize your templates. Parameters enable you to input custom values to your template each time you create or update a stack".

Option B is invalid since this is used to specify the Output values of a template

Option C is invalid since this is used to specify additional tags for the template

Option D is invalid since this is used to specify changes in a cloudformation template

For more information on Cloudformation parameters, please visit the below link

- https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html (https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/parameters-section-structure.html)

Ask our Experts 👍 👎

QUESTION 50 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are planning on creating a fault tolerant EC2 Instance by creating a secondary network interface and a backup EC2 Instance. Which of the following is a requirement to ensure the switch over can be done successfully? Choose 2 answers from the options given below

□ **A.** The network interface must reside in the same Availability Zone ✓

□ **B.** The network interface must reside in a different Availability Zone

□ **C.** The instance must reside in the same Availability Zone ✓

□ **D.** The instance must reside in a different Availability Zone

Explanation :

Answer – A and C
This is given in the AWS documentation
You can attach a network interface in one subnet to an instance in another subnet in the same VPC; however, both the network interface and the instance must reside in the same Availability Zone.
Options B and D are incorrect since the network interface must be in the same Availability Zone
For more information on Elastic Network Interfaces , please refer to the below URL

- http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html (http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html)

Ask our Experts 👍 👎

QUESTION 51 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You have a set of EC2 Instances created in a VPC. You need to ensure that logs from specific locations on the EC2 Instances are sent over to a central log location. How can you achieve this? Choose 2 answers from the options given below

□ **A.** Use the Cloudwatch logs agent ✓

□ **B.** Use the AWS Inspector agent

□ **C.** Centralize the logs to a Cloudwatch Log Group ✓

□ **D.** Centralize the logs to a VPC Log Group

Explanation :

Answer – A and C
The AWS Documentation mentions the following
To collect logs from your Amazon EC2 instances and on-premises servers into CloudWatch Logs, AWS offers both a new unified CloudWatch agent, and an older CloudWatch Logs agent. We recommend the unified CloudWatch agent. The new unified agent has the following advantages.

- You can collect both logs and advanced metrics with the installation and configuration of just one agent.
- The unified agent enables the collection of logs from servers running Windows Server.
- If you are using the agent to collect CloudWatch metrics, the unified agent also enables the collection of additional system metrics, for in-guest visibility.
- The unified agent provides better performance.

Option B is incorrect since the Inspector agent is only used to check for vulnerabilities
Option D is incorrect since the logs need to be aggregated in the VPC Log Group
For more information on Cloudwatch Logs agent , please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html (https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_GettingStarted.html)

Ask our Experts

QUESTION 52 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have a private subnet defined in a VPC. You have the requirement to ensure that instances can reach a server on the Internet. The responses from the external server needs to be relayed back to the private servers on pre-defined ports. How can you accomplish this.

○ **A.** Move the EC2 Instances to a public subnet

○ **B.** Install Squid Proxy on an EC2 Instance ✓

○ **C.** Use a NAT gateway in the public subnet

○ **D.** Use a NAT gateway in the private subnet

Explanation :

Answer – B

Since port forwarding is one of the key requirements, you cannot use a NAT gateway , you need to use a customized NAT instance
Option A is incorrect since the instance needs to remain in the private subnet
Options C and D are incorrect since we cannot use a NAT gateway in this circumstance.
For more information on the squid proxy , please refer to the below URL

- http://www.squid-cache.org/Intro/why.html (http://www.squid-cache.org/Intro/why.html)

Ask our Experts 👍 👎

QUESTION 53 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has setup an AWS Direct Connect connection from their on-premise location. An application in the on-premise location needs to access a DynamoDB table. All data written to Amazon DynamoDB should be encrypted as it is written to the database. How can you enable such a requirement?

○ **A.** Setup a private VIF

○ **B.** Setup a public VIF

○ **C.** Setup an IPSec VPN over a private VIF

○ **D.** Setup an IPSec VPN over a public VIF ✔

Explanation :

Answer – D
The AWS Documentation mentions the following
You can use AWS Direct Connect to establish a dedicated network connection between your network create a logical connection to public AWS resources, such as an Amazon virtual private gateway IPsec endpoint. This solution combines the AWS managed benefits of the VPN solution with low latency, increased bandwidth, more consistent benefits of the AWS Direct Connect solution, and an end-to-end, secure IPsec connection.
Options A and B are incorrect since just having a VIF alone will not work
Option C is incorrect since accessing a public resource such as DynamoDB , you need to have a public VIF
For more information on such a connectivity option , please refer to the below URL

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-direct-connect-plus-vpn-network-to-amazon.html)

Ask our Experts

QUESTION 54 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have created a load balancer in AWS with EC2 Instances behind them. The ELB is serving web traffic to users on the Internet. The Web servers behind the ELB are stateful web servers. Users begin to report intermittent connectivity issues when accessing the website. What can be done to ensure that the issue is resolved.

○ **A.** Ensure that the Security Group for the web servers are open on port 443

○ **B.** Ensure that the Security Group for the web servers are open for 0.0.0.0/0

○ **C.** Enable sticky sessions on the load balancer ✓

○ **D.** Enable connection draining

Explanation :

Answer – C
Option A is invalid because there is no mention of SSL in the question
Option B is invalid because you should not allow access from anywhere on the EC2 Instances
Option D is invalid because connection draining will not solve the issue.
The AWS Documentation mentions the following
Sticky sessions are a mechanism to route requests to the same target in a target group. This is useful for servers that maintain state information in order to provide a continuous experience to clients. To use sticky sessions, the clients must support cookies.
For more information on sticky sessions for the ELB , please refer to the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#sticky-sessions (https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-target-groups.html#sticky-sessions)

Ask our Experts

QUESTION 55 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your application hosted on AWS makes use of CloudHSM for getting SSL certificates. These certificates are installed on EC2 Instances behind an Autoscaling Group. How can you ensure that the CloudHSM modules are scaled along with the EC2 Instances for ensuring on time delivery of the SSL certificates.

○ **A.** Createa Network Load balancer and place the CloudHSM device behind it.

○ **B.** Justspecify the number of HSM modules in the cluster ✓

○ **C.** Createan Application Load balancer and place the CloudHSM device behind it.

○ **D.** Createanother Autoscaling Group for the CloudHSM modules

Explanation :

Answer – B
The AWS Documentation mentions the following
AWS CloudHSM provides hardware security modules (HSMs) in a *cluster*. A cluster is a collection of individual HSMs that AWS CloudHSM keeps in sync. You can think of a cluster as one logical HSM. When you perform a task or operation on one HSM in a cluster, the other HSMs in that cluster are automatically kept up to date.
You can create a cluster that has from 1 to 28 HSMs (the default limit is 6 HSMs per AWS account per AWS Region). You can place the HSMs in different Availability Zones in an AWS Region. Adding more HSMs to a cluster provides higher performance. Spreading clusters across Availability Zones provides redundancy and high availability.
Options A ,C and D are incorrect since the Load balancing capability already comes along with the cluster.
For more information on clusters in CloudHSM , please refer to the below URL

- https://docs.aws.amazon.com/cloudhsm/latest/userguide/clusters.html (https://docs.aws.amazon.com/cloudhsm/latest/userguide/clusters.html)

Ask our Experts

QUESTION 56 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You currently have a VPC which has a set of Instances. You now have a requirement to host an application in the VPC which primarily communicates on IPv6. What do you need to do to enable this requirement?

Select 2 answers.

□ **A.** Disable IPv4 for the subnet

□ **B.** Disable IPv4 for the VPC

□ **C.** Enable IPV6 for the subnet ✓

□ **D.** Enable IPV6 for the VPC ✓

Explanation :

Answer – C and D
The AWS Documentation mentions the following
If you have an existing VPC that supports IPv4 only, and resources in your subnet that are configured to use IPv4 only, you can enable IPv6 support for your VPC and resources. Your VPC can operate in dual-stack mode — your resources can communicate over IPv4, or IPv6, or both. IPv4 and IPv6 communication are independent of each other.
In order to enable to ipv6 on VPC and subnet level, we need to enable manually on VPC and subnet also. So, it looks like option C is also correct answer.

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html#vpc-migrate-ipv6-cidr (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html#vpc-migrate-ipv6-cidr)
Options A is incorrect since this setting is pertinent to the VPC
Option B is incorrect since you cannot disable IPv4 for the VPC
For more information on using Ipv6 , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-migrate-ipv6.html)

Ask our Experts 👍 👎

QUESTION 57 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You have Instances in a private subnet in a VPC. You have provisioned a NAT gateway in a public subnet to allow for instances in the private subnet to communicate with the Internet. You are trying to ping the Elastic IP of the NAT gateway from your workstation, but are not able to do so. What can be done to resolve this issue?

○ **A.** Change the Security Groups assigned to the NAT gateway to allow Incoming ICMP traffic

○ **B.** Change the NACL’s assigned to the public subnet hosting the NAT gateway to allow Incoming and outgoing ICMP traffic

○ **C.** Ping the public IP address of the NAT gateway instead of the Elastic IP

○ **D.** This is not possible , since this is how the NAT gateway works ✓

Explanation :

Answer – D
The AWS Documentation mentions the following to support this
NAT Gateway Doesn't Respond to a Ping Command
If you try to ping a NAT gateway's Elastic IP address or private IP address from the internet (for example, from your home computer) or from any instance in your VPC, you do not get a response. A NAT gateway only passes traffic from an instance in a private subnet to the internet.
To test that your NAT gateway is working, see Testing a NAT Gateway.
Option A is incorrect since there is no concept of Security Groups for NAT gateway’s
Option B is incorrect since changing the NACL’s is not the right approach
Option C is incorrect since the NAT gateway gets an Elastic IP
For more information on troubleshooting NAT gateways, please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html#nat-gateway-troubleshooting (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpc-nat-gateway.html#nat-gateway-troubleshooting)

Ask our Experts 👍 👎

QUESTION 58 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company has setup a series of EC2 Instances in a VPC. There is now a requirement to setup a management network inside of the VPC. Which of the following will be part of the implementation steps?

○ **A.** Attach multiple Elastic Network Interfaces to an Instance ✓

○ **B.** Attach multiple public IP addresses to an existing Elastic Network Interface for aninstance

○ **C.** Attach multiple Elastic IP addresses to an existing Elastic Network Interface for an instance.

○ **D.** Attach multiple private IP addresses to an existing Elastic Network Interface for aninstance

Explanation :

Answer – A
The AWS Documentation mentions the following to support this
Attaching multiple network interfaces to an instance is useful when you want to:

- Create a management network.
- Use network and security appliances in your VPC.
- Create dual-homed instances with workloads/roles on distinct subnets.
- Create a low-budget, high-availability solution.

All other options automatically are invalid since the primary implementation step is to create multiple ENI's
For more information on Elastic Network Interfaces , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ElasticNetworkInterfaces.html)

Creating a Management Network
You can create a management network using network interfaces. In this scenario, the primary network interface (eth0) on the instance handles public traffic and the secondary network interface (eth1) handles backend management traffic and is connected to a separate subnet in your VPC that has more restrictive access controls. The public interface, which may or may not be behind a load balancer, has an associated security group that allows access to the server from the internet (for example, allow TCP port 80 and 443 from *0.0.0.0/0*, or from the load balancer) while the private facing interface has an associated security group allowingSSH access only from an allowed range of IP addresses either within the VPC or from the internet, a private subnet within the VPC or a virtual private gateway.
To ensure failover capabilities, consider using a secondary private IPv4 for incoming traffic on a network interface. In the event of an instance failure, you can move the interface and/or secondary private IPv4 address to a standby instance.
For more information, please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#AvailableIpPerENI (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-eni.html#AvailableIpPerENI)

Ask our Experts 👍 👎

QUESTION 59 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You've setup a VPC peering connection between 2 VPC's , VPC A and VPC B. You are trying to ping the Instances in each VPC to each other. But you are not able to do so. You have verified the Security Groups for the Instances and the NACL's and confirmed that ICMP traffic is allowed. What steps need to be done to resolve the issue. Choose 2 answers from the options below.

□ **A.** Add a route in the route table in VPC A to VPC B via the VPC peering connection ✓

□ **B.** Add a route in the route table in VPC A to VPC B via the Internet gateway

□ **C.** Add a route in the route table in VPC B to VPC A via the VPC peering connection ✓

□ **D.** Add a route in the route table in VPC B to VPC A via the Internet gateway

Explanation :

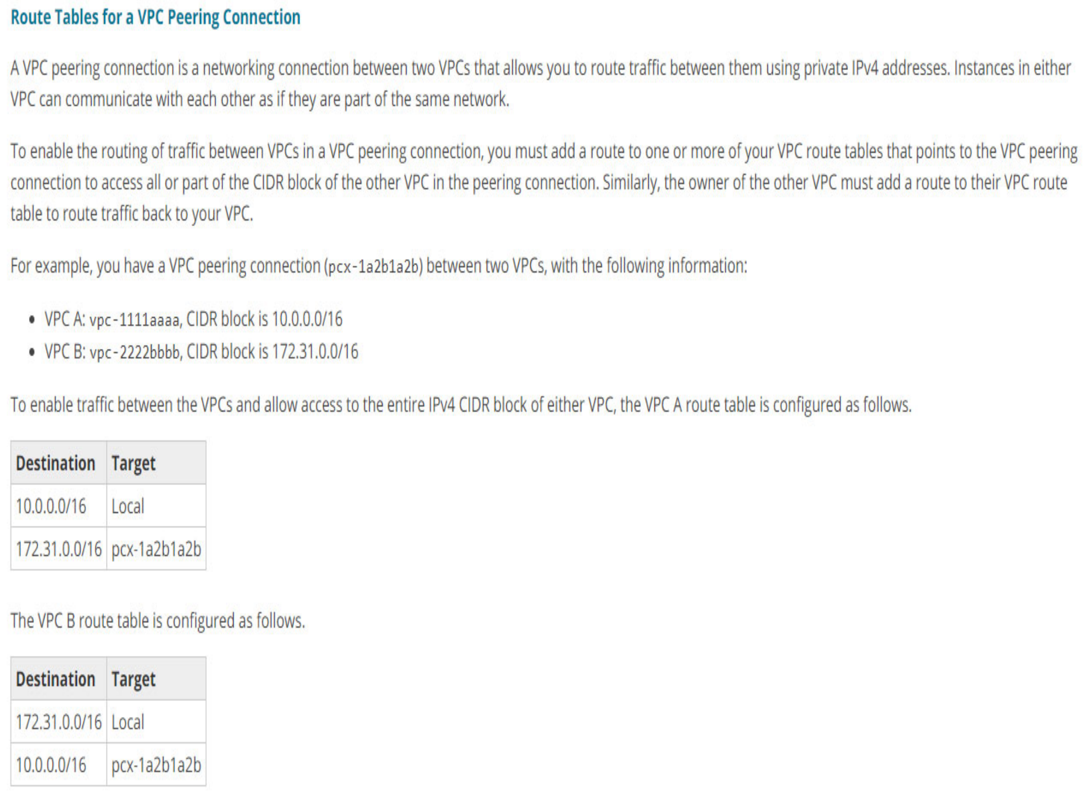
Answer – A and C
Options B and D are incorrect since the traffic should not move through the Internet gateway.
The AWS Documentation mentions the following to support this

Route Tables for a VPC Peering Connection

A VPC peering connection is a networking connection between two VPCs that allows you to route traffic between them using private IPv4 addresses. Instances in either VPC can communicate with each other as if they are part of the same network.
To enable the routing of traffic between VPCs in a VPC peering connection, you must add a route to one or more of your VPC route tables that points to the VPC peering connection to access all or part of the CIDR block of the other VPC in the peering connection. Similarly, the owner of the other VPC must add a route to their VPC route table to route traffic back to your VPC.
For example, you have a VPC peering connection (pcx-1a2b1a2b) between two VPCs, with the following information:

- VPC A: vpc-1111aaaa, CIDR block is 10.0.0.0/16
- VPC B: vpc-2222bbbb, CIDR block is 172.31.0.0/16

To enable traffic between the VPCs and allow access to the entire IPv4 CIDR block of either VPC, the VPC A route table is configured as follows.



Route Tables for a VPC Peering Connection

A VPC peering connection is a networking connection between two VPCs that allows you to route traffic between them using private IPv4 addresses. Instances in either VPC can communicate with each other as if they are part of the same network.

To enable the routing of traffic between VPCs in a VPC peering connection, you must add a route to one or more of your VPC route tables that points to the VPC peering connection to access all or part of the CIDR block of the other VPC in the peering connection. Similarly, the owner of the other VPC must add a route to their VPC route table to route traffic back to your VPC.

For example, you have a VPC peering connection (`pcx-1a2b1a2b`) between two VPCs, with the following information:

- VPC A: `vpc-1111aaaa`, CIDR block is 10.0.0.0/16
- VPC B: `vpc-2222bbbb`, CIDR block is 172.31.0.0/16

To enable traffic between the VPCs and allow access to the entire IPv4 CIDR block of either VPC, the VPC A route table is configured as follows.

Destination	Target
10.0.0.0/16	Local
172.31.0.0/16	pcx-1a2b1a2b

The VPC B route table is configured as follows.

Destination	Target
172.31.0.0/16	Local
10.0.0.0/16	pcx-1a2b1a2b

For more information on Route Tables for VPC Peering connections , please refer to the below URL

- https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vpc-peering (https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html#route-tables-vpc-peering)

Ask our Experts

QUESTION 60 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company has setup a host of networking components in AWS. They have out stringent controls in place to ensure that these networking components are only changed by designated IT personnel. But they still need to get notified of any unwarranted access on networking components. Which of the following service can help in this requirement?

○ **A.** AWS VPC Flow Logs

○ **B.** AWS Cloudtrail ✔

○ **C.** AWS Trusted Advisor

○ **D.** AWS Inspector

Explanation :

Answer – B
The AWS Documentation mentions the following
AWS CloudTrail provides a history of AWS API calls for an account, including API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). This AWS API call history enables security analysis, resource change tracking, and compliance auditing. Customers can also deliver CloudTrail data to CloudWatch Logs to store, monitor, and process API calls for network-specific changes and to send appropriate notifications. CloudTrail provides an AWS CloudFormation template to automatically create CloudWatch alarms for security- and network-related API activity.
Option A is incorrect since this can be used to monitor the traffic to the VPC
Option C is incorrect since this cannot be used to monitor changes to network resources
Option D is incorrect since this can only be used to perform vulnerability scan analysis on EC2 Instances
For more information on Networking management and monitoring , please refer to the below URL

- https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/ (https://aws.amazon.com/answers/networking/vpc-network-management-and-monitoring/)

Ask our Experts 👍 👎

QUESTION 61 **UNATTEMPTED**

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company has the following setup in AWS

a. A set of EC2 Instances hosting a web application

b. An application load balancer placed in front of the EC2 Instances

There seems to be a set of malicious requests coming from a set of IP addresses. Which of the following can be used to protect against these requests?

○ **A.** Use Security Groups to block the IP addresses

○ **B.** Use VPC Flow Logs to block the IP addresses

○ **C.** Use AWS Inspector to block the IP addresses

○ **D.** Use AWS WAF to block the IP addresses ✓

Explanation :

Answer – D
The AWS Documentation mentions the following on AWS WAF which can be used to protect Application Load Balancers and Cloud front
A web access control list (web ACL) gives you fine-grained control over the web requests that your Amazon CloudFront distributions or Application Load Balancers respond to. You can allow or block the following types of requests:

- Originate from an IP address or a range of IP addresses
- Originate from a specific country or countries
- Contain a specified string or match a regular expression (regex) pattern in a particular part of requests
- Exceed a specified length
- Appear to contain malicious SQL code (known as SQL injection)
- Appear to contain malicious scripts (known as cross-site scripting)

Option A is invalid because by default Security Groups have the Deny policy
Options B and C are invalid because these services cannot be used to block IP addresses
For information on AWS WAF, please visit the below URL

- https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html (https://docs.aws.amazon.com/waf/latest/developerguide/web-acl.html)

Ask our Experts 👍 👎

QUESTION 62 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You are planning on using VPC Flow logs to monitor the traffic to EC2 Instances in your VPC. Which of the following types of traffic will not get monitored by VPC Flow logs. Choose 2 answers from the options given below

□ **A.** Instances which have multiple ENI’s

□ **B.** Traffic that flow to Amazon DNS servers ✓

□ **C.** Instances that have Elastic IP’s assigned to the ENI

□ **D.** Requests for instance metadata ✓

Explanation :

Answer – B and D

The AWS Documentation mentions the following

The Flow Logs will not include any of the following traffic:

1. Traffic to Amazon DNS servers, including queries for private hosted zones.
2. Windows license activation traffic for licenses provided by Amazon.
3. Requests for instance metadata.
4. DHCP requests or responses.

Based on the above information , all other information becomes invalid

For information on VPC Flow Logs please visit the below URL

- https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/ (https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/)

Ask our Experts 👍 👎

QUESTION 63 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You've setup a Cloudfront distribution in AWS. You're planning on conducting a primary load test to see the performance of the Cloudfront distribution. Which of the following factors must you keep in mind when performing the load test. Choose 2 answers from the options given below

□ **A.** Ensure to initiate client requests from multiple geographic regions ✓

□ **B.** Configure your test so each client makes an independent DNS request ✓

□ **C.** Ensure that client requests hit the origin server

□ **D.** Ensure that SSL is turned on for the distribution

Explanation :

Answer – A and B

The AWS Documentation mentions the following

CloudFront is designed to scale for viewers that have different client IP addresses and different DNS resolvers across multiple geographic regions. To perform load testing that accurately assesses CloudFront performance, we recommend that you do all of the following:

- Send client requests from multiple geographic regions.
- Configure your test so each client makes an independent DNS request; each client will then

receive a different set of IP addresses from DNS.

· For each client that is making requests, spread your client requests across the set of IP addresses that are returned by DNS, which ensures that the load is distributed across multiple servers in a CloudFront edge location.

Option C is incorrect since you need to initiate the request to the Cloudfront distribution
Option D is incorrect since there is no mention of a secure request in the question.
For information on Load Testing with Cloudfront, please visit the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/load-testing.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/load-testing.html)

Ask our Experts 👍 👎

QUESTION 64 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company currently has the following requirement

Transfer of data from an on-premise Hadoop cluster on AWS
The transfer of data can run into 1Gbps to 1.5Gbps
Requirement for consistent and fault tolerant data transfer on AWS
Which of the following would you incorporate?

○ **A.** A single 1 Gbps AWS Direct Connect connection with a AWS VPN backup

○ **B.** Two 1 Gbps AWS Direct Connect connection with a AWS VPN backup

○ **C.** Three 1 Gbps AWS Direct Connect connection ✔

○ **D.** Two 1 Gbps AWS Direct Connect connection with two AWS VPN backup

Explanation :

Answer – C
You will need 3 AWS Direct Connect connection. 2 of them will be for normal data transfer. The third one will be a backup incase any connection fails.
All other options are incorrect because AWS VPN does not give consistent data transfers
For information on AWS Network connectivity, please visit the below URL

- https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/ (https://aws.amazon.com/answers/networking/aws-multiple-data-center-ha-network-connectivity/)

Ask our Experts

QUESTION 65 CORRECT DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company is planning on using AWS EC2 and ELB for deployment for their web applications. The security policy mandates that all traffic should be encrypted. Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

☐ **A.** Ensure the load balancer listens on port 80

☑ **B.** Ensure the load balancer listens on port 443 ✓

☑ **C.** Ensure the HTTPS listener sends requests to the instances on port 443 ✓

☐ **D.** Ensure the HTTPS listener sends requests to the instances on port 80

Explanation :

Answer - B and C
The AWS Documentation mentions the following
You can create a load balancer that listens on both the HTTP (80) and HTTPS (443) ports. If you specify that the HTTPS listener sends requests to the instances on port 80, the load balancer terminates the requests and communication from the load balancer to the instances is not encrypted. If the HTTPS listener sends requests to the instances on port 443, communication from the load balancer to the instances is encrypted.
Option A is invalid because there is a need for secure traffic , so port 80 should not be used
Option D is invalid because for the HTTPS listener you need to use port 443
For more information on HTTPS with ELB, please refer to the below link

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-create-https-ssl-load-balancer.html)

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14783)

Certification

- Cloud Certification (https://www.whizlabs.com/cloud-certification-training-courses/)
- Java Certification (https://www.whizlabs.com/oracle-java-certifications/)
- PM Certification (https://www.whizlabs.com/project-management-certifications/)
- Big Data Certification (https://www.whizlabs.com/big-data-certifications/)

Company

- Support (https://help.whizlabs.com/hc/en-us)
- Discussions (http://ask.whizlabs.com/)
- Blog (https://www.whizlabs.com/blog/)

Mobile App

Android Coming Soon

iOS Coming Soon

Follow us

f

(https://www.facebook.com/whizlabs.software/)

in

(https://in.linkedin.com/company/whizlabs-software)

(https://twitter.com/whizlabs?lang=en)

G+

(https://plus.google.com/+WhizlabsSoftware)