NEW PRACTICE TEST III

Attempt	1
Marks Obtained	0 / 65
Your score is	0.0%

Completed on	Sunday , 03 February 2019 , 12:28 AM
Time Taken	00 H 01 M 16 S
Result	Fail

Domains / Topics wise Quiz Performance Report

S.No.	Topic	Total Questions	Correct	Incorrect	Unattempted
1	Design and implement hybrid IT network architectures at scale	13	0	1	12
2	Design and implement for security and compliance	7	0	1	6
3	Design and implement AWS networks	22	0	0	22
4	Manage, optimize, and troubleshoot the network	15	0	0	15
5	Configure network integration with application services	7	0	0	7
6	Automate AWS tasks	1	0	0	1

65 Questions	0 Correct	2 Incorrect	63 Unattempted

Show Answers

All

QUESTION 1 INCORRECT

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company is planning on setting up a Direct Connect connection to AWS. But they don't require or have the facility to accommodate a 1Gbps connection. How can they achieve a sub 1G connection? Choose 2 answers from the options given below.

- [ ] **A.** If they have a parent AWS Account which can accommodate a 1G connection , look at having a Hosted Virtual Interface ✔
- [x] **B.** If they have a parent AWS Account which can accommodate a 1G connection , look at having a Hosted Connection ✖
- [x] **C.** They can consider contacting an AWS Partner for a Hosted Virtual Interface ✖
- [ ] **D.** They can consider contacting an AWS Partner for a Hosted Connection ✔

Explanation :

Answer – A and D

Below are the options as given in the AWS Documentation

Hosted virtual interfaces (VIF) Hosted virtual interfaces (VIF) can connect to public resources or a VPC in the same way as standard VIFs, except that the account that owns the hosted VIF is different from the connection owner. Bandwidth is shared across all virtual interfaces on the parent connection.

Hosted connections allow an APN partner to create a Direct Connect sub-1G connection for you, allocating dedicated bandwidth for that connection rather than having multiple VIFs on the same parent connection competing for bandwidth.

Option B is incorrect because you need to have a Hosted Virtual Interface with a parent AWS account
Option C is incorrect because you need to have a Hosted Connection with an AWS Partner
For more information on the Direct Connect types , please visit the following URL

- https://aws.amazon.com/premiumsupport/knowledge-center/direct-connect-types/ (https://aws.amazon.com/premiumsupport/knowledge-center/direct-connect-types/)

Ask our Experts

QUESTION 2 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

A Company currently uses the NetFlow software to monitor and get the details of the traffic that flows between systems in their On-premise network. They want to have the same ability when they start moving their servers to AWS. Which of the following service can help them meet this requirement.

- A. AWS Cloudwatch logs
- B. AWS VPC Flow Logs ✔
- C. AWS Cloudwatch metrics
- D. AWS Config

Explanation :

Answer – B
NetFlow is a network protocol developed by Cisco for collecting IP traffic information and monitoring network traffic.
The AWS Documentation mentions the following

VPC Flow Logs are similar to scheduled NetFlow/sFlow/IPFIX reports. Flow logs collect the source and destination IP, source and destination ports, protocol, packet counts, and ALLOW or DENY action for a particular VPC, subnet, or ENI. They are currently collected and sent as a report every 10 minutes.
Options A,C and D are all incorrect because the right software which matches the Netflow software is VPC Flow Logs
For more information on VPC Flow logs , please visit the following 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 3 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

A company has an application that needs to be moved to an AWS VPC network. This application is based on multicast and needs to be moved with the least amount of effort. What can be done to fulfil this requirement?

- **A.** Create EC2 Instances in the subnet and then migrate the application on to the EC2 Instance.
- **B.** The application needs to be changed to support unicast before moving it to AWS.
- **C.** Consider creating an overlay network between EC2 Instances and then port the application. ✔
- **D.** Consider enabling encryption on the underlying EBS volumes which will be used to support the EC2 Instance

Explanation :

Answer – C

Currently Amazon VPC service doesn't presently permit multicast or broadcast traffic. In the event that you have an application that uses multicast to function, you can leverage GRE tunnels to create a mesh VPN overlay network between your Amazon EC2 instances

Option A is incorrect because you need to setup an overlay network first

Option B is incorrect because this would be a major change for the application.

Option D is incorrect because this would not help in the requirement

An example of a vendor that can provide an overlay network is given below

- https://aws.amazon.com/marketplace/pp/B071RMCZ1X (https://aws.amazon.com/marketplace/pp/B071RMCZ1X)

Ask our Experts

QUESTION 4 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

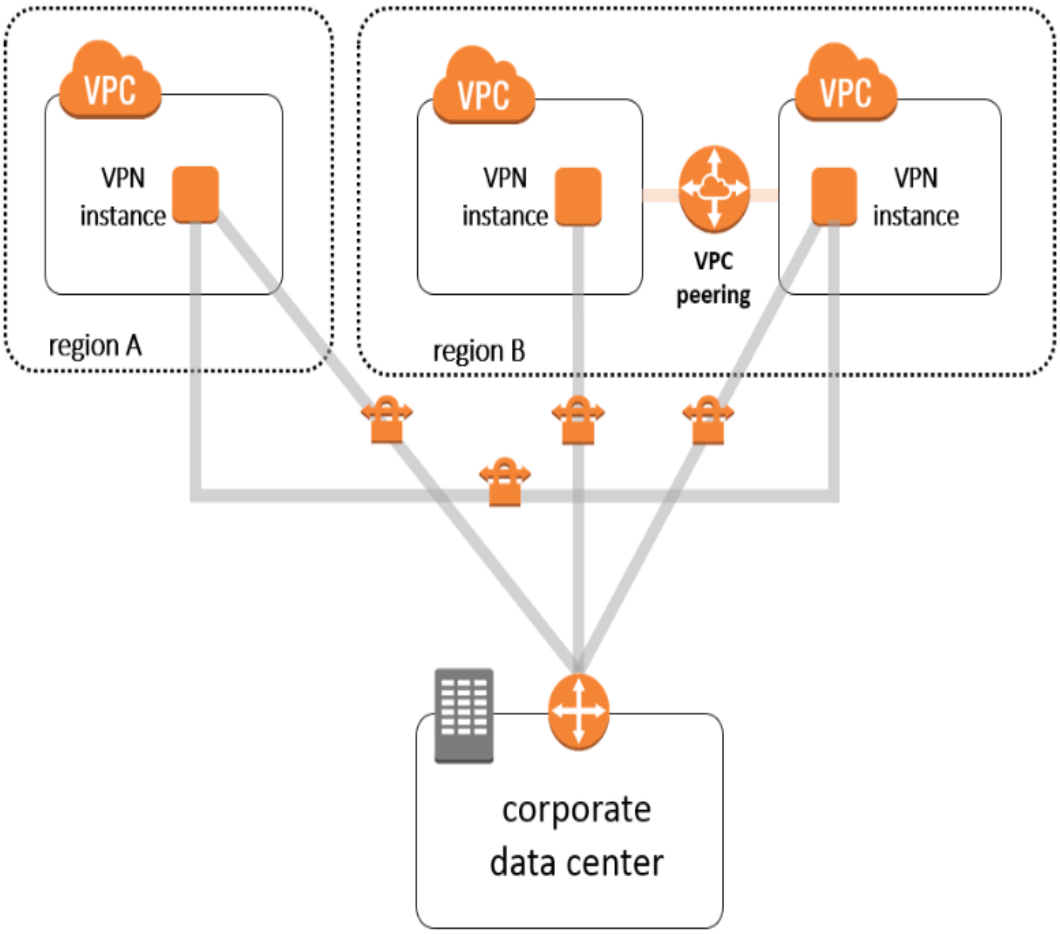
A company currently has acquired another smaller company. Both companies have their presence in AWS. There is a requirement to ensure traffic flows from VPC A in the parent company to a security VPC B in the same parent company. And then the traffic can flow to VPC C in the acquired company. How can you accomplish this transit flow?

- **A.** Create a VPC Peering connection between VPC A and VPC B. Create another VPC peering connection between VPC B and VPC C
- **B.** Create a VPC Peering connection between VPC A and VPC C. Create another VPC peering connection between VPC B and VPC C
- **C.** Create a VPC Peering connection between VPC A and VPC B. Create a VPN connection between VPC B and VPC C ✔
- **D.** Create a VPC Peering connection between VPC A and VPC C. Create a VPN connection between VPC A and VPC B

Explanation :

Answer – C

A sample architecture diagram of such a setup is given below



You can peer VPC A and VPC B. And then traffic can flow to VPC C via a VPN device setup on an EC2 Instance

Options A and B are incorrect because transitive routing is not allowed

Option D is incorrect since the VPC connection should be established between VPC B and C.

For more information on transit networks , please refer to the below URL

https://aws.amazon.com/answers/networking/aws-global-transit-network/ (https://aws.amazon.com/answers/networking/aws-global-transit-network/)

Ask our Experts

QUESTION 5 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are setting up a VPN software on an EC2 Instance which will be used for VPN connections. Which of the following is an important aspect that should be set on the EC2 Instance?

- A. Disable source destination check on the Amazon EC2 instance. ✔
- B. Enable source destination check on the Amazon EC2 instance.
- C. Enable route propagation in a Virtual Private Cloud (VPC) subnet route table.
- D. Enable enhanced networking mode on the Amazon EC2 instance.

Explanation :

Answer – A

Option B is incorrect since the source destination check on the Amazon EC2 instance should be disabled.

Option C is incorrect since this is required for Amazon provided VPN connections

Option D is incorrect since this is not a primary requirement

You have Disable source destination check on the Amazon EC2 instance. An example is also given in the AWS Documentation

To launch an EC2 VPN instance

1.Launch an Amazon Linux instance in a VPC public subnet and do the following:

a)Assign the VPN instance a static private IP address. This is not required, but it makes setting up the config files easier. In this example, use 10.0.0.5.

b)Allocate a VPC EIP and associate an EIP to your VPN instance. In this example, use EIP1 to represent the public EIP address used to connect into your VPC.

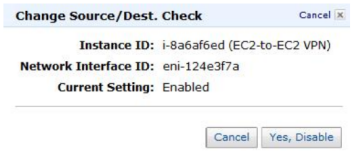
2. Disable Source/Dest checking on your EC2 instance.

a)Right-click the instance and selecting Change Source/Dest. Check.

b)Click Yes, Disable.

To launch an EC2 VPN instance

1. Launch an Amazon Linux instance in a VPC public subnet and do the following:
   a. Assign the VPN instance a static private IP address. This is not required, but it makes setting up the config files easier. In this example, use 10.0.0.5.
   b. Allocate a VPC EIP and associate an EIP to your VPN instance. In this example, use EIP1 to represent the public EIP address used to connect into your VPC.
2. Disable Source/Dest checking on your EC2 instance.
   a. Right-click the instance and selecting **Change Source/Dest. Check.**
   b. Click **Yes, Disable**.



For more an example on setting up a VPN software on an EC2 Instance, please refer to the below URL

- https://aws.amazon.com/articles/connecting-cisco-asa-to-vpc-ec2-instance-ipsec/ (https://aws.amazon.com/articles/connecting-cisco-asa-to-vpc-ec2-instance-ipsec/)

Ask our Experts

QUESTION 6 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

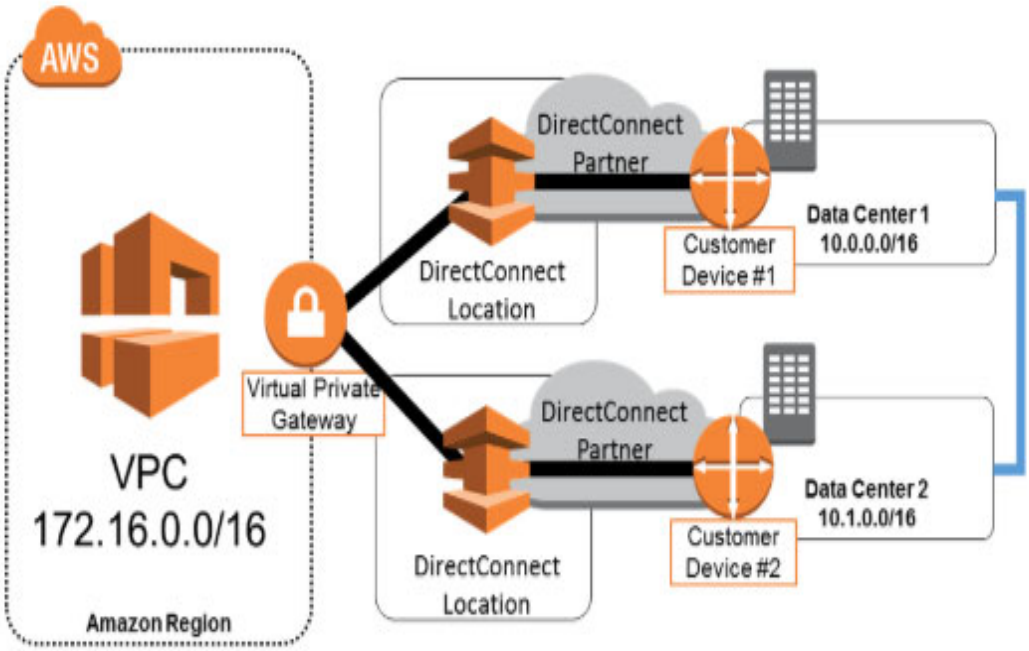
Your company is planning on setting up an AWS Direct connect connection to an AWS VPC. They want to achieve maximum fault tolerance , have maximum bandwidth at all times. How can this be achieved?

- **A.** One Virtual Private gateway Two AWS Direct Connect Locations Two Customer gateways ✔
- **B.** Two Virtual Private gateway Two AWS Direct Connect Locations One Customer gateway

- **C.** Two Virtual Private gateway One AWS Direct Connect Location One Customer gateway
- **D.** One Virtual Private gateway One AWS Direct Connect Location One VPN connection Two Customer gateways

Explanation :

Answer – A
Options B and C are incorrect because there should only be one Virtual Private gateway
Option D is incorrect because since you need maximum bandwidth at all times , having a backup VPN is not preferred.
The below architecture diagram from the AWS Documentation mentions how this high availability can be achieved.



For more information on high network connectivity , please refer to 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 7 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company currently has a VPC hosted in AWS. There is a private hosted zone in place for the instances in this VPC. You need your On-premise servers to be able to resolve DNS requests for instances in the VPC. You need to do this with the least amount of effort. What steps would you. Choose 2 answers from the options given below.

- [x] **A.** Setup a Simple AD Instance in AWS. ✔
- [ ] **B.** Setup an Active Directory Domain Controller in the AWS VPC
- [x] **C.** Make your On-premise servers point to the Simple AD Instance ✔
- [ ] **D.** Make your On-premise servers point to the new Domain Controller

Explanation :

Answer – A and C

Options B and D are invalid , because even though feasible would require more effort to setup.

The AWS Documentation mentions the following

Simple AD forwards DNS requests to the IP address of the Amazon-provided DNS servers for your VPC. These DNS servers will resolve names configured in your Route 53 private hosted zones. By pointing your on-premises computers to your Simple AD, you can now resolve DNS requests to the private hosted zone.

For more information on Simple AD , please refer to the below URL

- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/simple_ad_dns.html (https://docs.aws.amazon.com/directoryservice/latest/admin-guide/simple_ad_dns.html)

Ask our Experts

QUESTION 8 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You've currently configured health checks in Route 53. These health checks are being used for 2 of your on-premise web servers. The health checks are not working as desired. The health checks are continually failing. Which of the following could be a possible reason?

- A. Ensure that the Security groups on the Instances are allowing Inbound Traffic
- B. Ensure that the NACL's on the Subnets are allowing Inbound Traffic
- C. Ensure that the Firewall on your On-premise environment is allowing Inbound Traffic ✔
- D. This is not possible. You cannot enable health checks for non-AWS resources

Explanation :

Answer – C
The AWS Documentation mentions the following
When Route 53 checks the health of an endpoint, it sends an HTTP, HTTPS, or TCP request to the IP address and port that you specified when you created the health check. For a health check to succeed, your router and firewall rules must allow inbound traffic from the IP addresses that the Route 53 health checkers use.
Options A and B are invalid because the health checks are not being configured for EC2 Instances
Option D is incorrect because it is possible to use AWS Route 53 for monitoring non-AWS resources
For more information on Route 53 health checks , please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-router-firewall-rules.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-failover-router-firewall-rules.html)

Ask our Experts

QUESTION 9 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You are currently configuring Route 53 routing policies. You want to create a record set for a group of Web servers in your AWS VPC. When a user requests for the resource record , they should be able to access any of the web servers defined in the VPC. Which of the following resource record would you create?

- A. Simple
- B. Weighted
- C. Failover
- D. Multivalue answer ✔

Explanation :

Answer – D

Options A,B and C are invalid because for such a requirement , you have to use the Multivalue answer resource record

The AWS Documentation mentions the following

Multivalue answer routing lets you configure Amazon Route 53 to return multiple values, such as IP addresses for your web servers, in response to DNS queries. You can specify multiple values for almost any record, but multivalue answer routing also lets you check

the health of each resource, so Route 53 returns only values for healthy resources. It's not a substitute for a load balancer, but the ability to return multiple health-checkable IP addresses is a way to use DNS to improve availability and load balancing.
For more information on Routing policy's , please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html)

Ask our Experts

QUESTION 10 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your team is planning on creating a set of instances in a VPC. They need to ensure high network performance for the underlying instances and enhanced communication between the instances. Which of the following steps would you take. Choose 2 answers from the options given below

- [ ] **A.** Enable Enhanced Networking for the underlying Instances ✔
- [ ] **B.** Set the MTU for the Instances to 1500
- [ ] **C.** Create the Instances in separate Availability Zones and put them in a cluster placement Group
- [ ] **D.** Create the Instances in the same Availability Zones and put them in a cluster placement Group ✔

Explanation :

Answer – A and D
The AWS Documentation mentions the following

A cluster placement group is a logical grouping of instances within a single Availability Zone. Placement groups are recommended for applications that benefit from low network latency, high network throughput, or both. To provide the lowest latency, and the highest packet-per-second network performance for your placement group, choose an instance type that supports enhanced networking
Option B is invalid because this is the default MTU available
Option C is invalid because the instances need to be in the same available zone for being part of a placement group
For more information on Placement groups , please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html (https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html)

Ask our Experts

QUESTION 11 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You are trying to send packets from an EC2 Instance to an on-premise server. The transmission is happening over the Internet. You have set Jumbo frames due to the size of the packets being sent. But the packets are being dropped. What needs to be done to ensure that the packets don't get dropped?

- **A.** Ensure that the MTU is set to 9001
- **B.** Ensure that the "Do Not Fragment" flag is set in the IP header
- **C.** Ensure that the "Do Not Fragment" flag is not set in the IP header ✔
- **D.** Enable Enhanced Networking on the Instance

Explanation :

Answer – C
The AWS Documentation mentions the following
Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, outside of a given AWS region (EC2-Classic), a single VPC, or a VPC peering connection, you will experience a maximum path of 1500 MTU. VPN connections and traffic sent over an Internet gateway are limited to 1500 MTU. If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don't Fragment flag is set in the IP header.
Option B is invalid because this would lead to dropping frames
Option A is invalid because this is equivalent to Jumbo frames
Option D is invalid because this would not resolve the issue
For more information on Network MTU , please refer to the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/network_mtu.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/network_mtu.html)

Ask our Experts

QUESTION 12 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You're hosting an NGINX web server running on port 80 on an EC2 Instance. Users are not able to access the server running on port 80. Which of the following could be an issue

- A. The Security Group does not allow outbound traffic on port 80
- B. The NACL don't allow outbound traffic on ephemeral ports ✔
- C. The NACL don't allow inbound traffic on ephemeral ports
- D. The Security Group does not allow inbound traffic on ephemeral ports

Explanation :

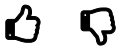
Answer – B
Options A and C are incorrect because the Security Group should only allow inbound traffic on port 80.
Option C is incorrect because it should be the outbound traffic for ephemeral ports
When a connection is established on a client , you need to ensure that outbound traffic is enabled on any ephemeral ports for the client.
This is also given in the AWS Documentation

Ephemeral Ports

The example network ACL in the preceding section uses an ephemeral port range of 32768-65535. However, you might want to use a different range for your network ACLs depending on the type of client that you're using or with which you're communicating. 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.
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 13 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company is planning on moving its files from its on-premise location onto S3. The services hosted in the on-premise environment would need low latency access to these files. Which of the following is the most secure way to have this established?

- A. Create a VPN connection which would allow the services on-premise to access S3
- B. Create a Direct Connect connection along with a Public VIF ✔
- C. Create a Direct Connect connection along with a Private VIF
- D. Create a VPN connection along with a VPC endpoint

Explanation :

Answer – B
This is also given in the AWS Documentation
To connect to AWS public endpoints, such as an Amazon Elastic Compute Cloud (Amazon EC2) or Amazon Simple Storage Service (Amazon S3), with dedicated network performance, use a public virtual interface.
Option A is invalid since VPN connections don't ensure low latency
Option C is invalid since you need to have a Public VIF for public services such as S3
Option D is invalid since VPV endpoints is invalid in this configuration
For more information on Public and Private Virtual Interfaces , please refer to the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/ (https://aws.amazon.com/premiumsupport/knowledge-center/public-private-interface-dx/)

Ask our Experts

QUESTION 14 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have a set of Instances in your VPC that communicate over the IPv6 protocol. You need to ensure that traffic can flow from the Instances to the Internet but not vice versa. How ca you achieve this.

- **A.** Change the Internet gateway to only allow outbound traffic for IPv6
- **B.** Change the Security Groups to not allow Inbound Traffic on the Instances
- **C.** Change the NACL's to not allow Inbound Traffic on the Instances
- **D.** Use an Egress only Internet gateway ✔

Explanation :

Answer – D
This is also given in the AWS Documentation
IPv6 addresses are globally unique, and are therefore public by default. If you want your instance to be able to access the Internet, but you want to prevent resources on the Internet from initiating communication with your instance, you can use an egress-only Internet gateway. To do this, create an egress-only Internet gateway in your VPC, and then add a route to your route table that points all IPv6 traffic (::/0) or a specific range of IPv6 address to the egress-only Internet gateway. IPv6 traffic in the subnet that's associated with the route table is routed to the egress-only Internet gateway.
Option A is invalid since there is no such option
Options B and C are invalid since this is not the right way to limit traffic for IPv6 for such a requirement
For more information on Egress only Internet gateway , please refer to the below URL

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

Ask our Experts

QUESTION 15 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You currently have setup a VPN configuration from your on-premise location to AWS. Your AWS VPC has a CIDR of 10.0.0.0/16 and a subnet of 10.0.1.0/24. Your On-premise location has a network of CIDR block of 10.0.37.0/24. The traffic is being dropped when it is being sent from the subnet instances to your on-premise location. Why could be the most probable reason in this case?

- A. You have not set Enhanced Networking on the Instances
- B. There is an overlap in prefixes ✔
- C. The "Do not fragment" is set in the IP header
- D. The MTU is not set to 9001

Explanation :

Answer – B

Such an example is given in the AWS Documentation

Connections with Your Local Network and Other VPCs

You can optionally set up a connection between your VPC and your corporate or home network. If you have an IPv4 address prefix in your VPC that overlaps with one of your networks' prefixes, any traffic to the network's prefix is dropped. For example, let's say that you have the following:

- A VPC with CIDR block 10.0.0.0/16
- A subnet in that VPC with CIDR block 10.0.1.0/24
- Instances running in that subnet with IP addresses 10.0.1.4 and 10.0.1.5
- On-premises host networks using CIDR blocks 10.0.37.0/24 and 10.1.38.0/24

When those instances in the VPC try to talk to hosts in the 10.0.37.0/24 address space, the traffic is dropped because 10.0.37.0/24 is part of the larger prefix assigned to the VPC (10.0.0.0/16). The instances can talk to hosts in the 10.1.38.0/24 space because that block isn't part of 10.0.0.0/16.

Options A,C and D are incorrect as there is no suggestions in the question on the type of

traffic that is being sent.
For more information on VPC and Subnets , please refer to the below URL

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

Ask our Experts

QUESTION 16 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company is planning on creating a Direct Connect connection and also have a VPN as a backup connection. Which of the following must be done to ensure that the AWS Direct connect connection is the preferred path?

- **A.** Ensure that prefixes are advertised the same on both connections ✔
- **B.** Ensure that the longest prefix is advertised on AWS Direct connect
- **C.** Ensure that AS_PATH prepending is configured on AWS Direct Connect
- **D.** Ensure that the shortest prefix is advertised on AWS Direct connect

Explanation :

Answer – A
By default , AWS will choose AWS Direct Connect. In order to ensure architecture for proper failover the AWS Documentation mentions the following points
To configure the hardware VPN as a backup for your Direct Connect connection:

· Be sure that you use the same virtual private gateway for both Direct Connect and the VPN connection to the VPC.
· If you are configuring a Border Gateway Protocol (BGP) VPN, advertise the same prefix for Direct Connect and the VPN.
· If you are configuring a static VPN, add the same static prefixes to the VPN connection

that you are announcing with the Direct Connect virtual interface.

· If you are advertising the same routes toward the AWS VPC, the Direct Connect path is always be preferred, regardless of AS path prepending.

Options B,C and D are incorrect because these are not the right configurations when configuring an active/passive connection with AWS Direct Connect and AWS VPN.
For more information on these points , please refer to the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/ (https://aws.amazon.com/premiumsupport/knowledge-center/configure-vpn-backup-dx/)

Ask our Experts

QUESTION 17 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on trying out AWS Workspaces for 100 users. They want to use a directory service along with AWS workspaces. Which of the following would be the ideal option which will have a least administrative overhead and also be cost effective.

- **A.** Deploy an AD domain server in a VPC and configure AWS Workspace to use the newly created AD Domain server
- **B.** Choose an AD connector to use along with AWS Workspaces
- **C.** Choose Simple AD to use along with AWS Workspaces ✔
- **D.** Choose AWS Directory Service to use along with AWS Workspaces

Explanation :

Answer – C
The AWS Documentation mentions the following

Amazon WorkSpaces uses directories to store and manage information for your WorkSpaces and users. For your directory, you can choose from Simple AD, AD Connector, or AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as Microsoft AD. In addition, you can establish a trust relationship between your Microsoft AD directory and your on-premises domain.
Option A is incorrect because this would require more effort
Option B is incorrect because there is no mention of an existing Director Service to use along with the AD connector
Option D is incorrect because this would not be cost effective
For more information on Simple AD with AWS workspaces , please refer to the below URL

- https://docs.aws.amazon.com/workspaces/latest/adminguide/launch-workspace-simple-ad.html (https://docs.aws.amazon.com/workspaces/latest/adminguide/launch-workspace-simple-ad.html)

Ask our Experts

QUESTION 18 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company currently has a VPC defined as 10.0.0.0/16. Subnets are defined in this VPC along with Instances created in the subnet. You need to ensure that resources in the VPC can resolve your on-premise DNS resources. How can you achieve this? Choose 2 answers from the options given below.

- [ ] **A.** Create an EC2 Instance in your VPC which will act as the DNS server ✔
- [ ] **B.** Configure DHCP Options for your VPC to point to the EC2 Instance. ✔
- [ ] **C.** Configure DHCP Options for your Subnet to point to the EC2 Instance.

☐ **D.** Create a private hosted zone in Route53

Explanation :

Answer – A and B
Here you can create your own EC2 Instance which will act as the DNS server. The VPC can then use the DHCP Options which points to this EC2 Instance as the DNS resolver.
Option C is incorrect because the DHCP options set is tagged with the VPC and not the subnet
Option D is incorrect because the private hosted zone should be used with routing requests in the VPC
For more information on DNS in a VPC , please refer to the below URL

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

Ask our Experts

QUESTION 19 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You need to setup an EC2 Instance in a VPC. This EC2 needs to ensure that it can communicate both with a private and public subnet which are located in the same availability zone. Traffic in the private subnet can only be sent to this central EC2 Instance. How can you achieve this?

○ **A.** Assign a secondary IP to the ENI attached to the EC2 Instance

○ **B.** Attach a public and private IP to the instance

○ **C.** Attach an elastic IP to the Instance

○ **D.** Attach a secondary ENI to the Instance ✔

Explanation :

Answer - D

The Instance in the question is going to behave as a management instance. In such a case you can separate ENI's , one for each subnet

This is also given as a scenario in the AWS Documentation

Scenarios for Network Interfaces

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.

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 allowing SSH 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.

Options A,B and C are incorrect since none of these options will help accomplish the requirement.

For more information on using the Elastic Network Interface, please refer to the below URL

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

Ask our Experts

QUESTION 20 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You're planning on creating a VPN connection to 2 VPC's in AWS. You are going to be using the same customer gateway in both cases. These VPC's have overlapping CIDR blocks. What can be done to ensure the routing is done right on the customer side.

- A. Use static routes on the customer side
- B. Configure AS_PATH for each of the routes
- C. Use VRF technology for routing ✔
- D. Use BFD technology for routing

Explanation :

Answer – C
This is given in the AWS Documentation
Virtual Routing and Forwarding (VRF) is a technology that allows multiple instances of a routing table to co-exist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. AWS recommends using VRFs when connecting a single customer gateway to multiple Amazon VPCs because the VPN connection creation logic is designed to ensure unique tunnel IP addresses for each connection within a single VPC, but not necessarily across multiple VPCs.
Options A and B are incorrect since these would not help in routing
Option D is incorrect because this used for failover connections
For more information on configuring routes to multiple VPC's , please refer to the below URL

- https://aws.amazon.com/articles/connecting-a-single-customer-router-to-multiple-vpcs/ (https://aws.amazon.com/articles/connecting-a-single-customer-router-to-multiple-vpcs/)

Ask our Experts

QUESTION 21 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You have created a NAT gateway to ensure that instances in your private subnet can download updates from the internet. But the instances are still not able to reach the internet even after the gateway has been created. Which of the following could be one of the underlying issue?

- A. The NAT gateway has not been created with the wrong AMI
- B. The NAT gateway has been created in the public subnet
- C. The NAT gateway has been created with the wrong Instance type
- D. The NAT gateway has been created in the private subnet ✔

Explanation :

Answer – D
Options A and C are incorrect because this is relevant when you are creating NAT Instances
Option B is incorrect since the NAT gateway should be created in the public subnet
The AWS Documentation mentions the following
To troubleshoot instances that can't connect to the Internet from a private subnet using a NAT gateway, check the following:

- Verify that the destination is reachable by pinging the destination from another source using a public IP address.
- Verify that the NAT gateway is in the Available state. Note: A NAT gateway in the Failed state is automatically deleted after about an hour.
- Make sure that you've created your NAT gateway in a public subnet, and that that the public route table has a default route pointing to an Internet gateway.
- Make sure that the private subnet's route table has a default route pointing to the NAT gateway.

Check that you have allowed the required protocols and ports for outbound traffic to the Internet.

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

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

Ask our Experts

QUESTION 22 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have an application that consists of the following setup

· An EC2 Instance that supports the main front end part of the application

· An EC2 Instance that is used to process Images

You are planning on using a load balancer to route requests based on the type of request and then route them to the respective servers. How can you accomplish this? Choose 2 answers from the options given below

- [ ] **A.** Create a Classic load balancer
- [ ] **B.** Create an Application load balancer ✔
- [ ] **C.** Create a TCP listener
- [ ] **D.** Create different target groups ✔

Explanation :

Answer – B and D

Here you need to route traffic based on the type of URL request. So based on the URL request , the request could go to either EC2 Instance. For this you need to create an Application Load balancer and target groups for each EC2 Instance

Options A and C are incorrect because a Classic Load Balancer would not help in this case.

For more information on Application Load Balancers , 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 23 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

Your company is planning on setting up applications with the following aspects

- 2 Applications , each with their own domain name
- Each application will have EC2 Instances as Web servers

You need to ensure High Availability for the servers and also configure Route53. How would you achieve this? Choose 2 answers from the options given below

- ☐ **A.** Configure 2 private hosted zones in Route 53
- ☐ **B.** Configure 2 public hosted zones in Route 53 ✔
- ☐ **C.** Create a public Elastic Load Balancer ✔
- ☐ **D.** Create a private Elastic Load Balancer

Explanation :

Answer – B and C
Since 2 domains are required , and hence since these are Web servers which most probably will need to be exposed to the Internet, you need to define 2 separate public hosted zones and 2 ELB's.
Options A and D are incorrect since private zones and ELB's will not allow access to the resources from the Internet
For more information on working with Hosted Zones , please refer to the below URL

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

Ask our Experts

QUESTION 24 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company has set EC2 Instances in a VPC. These Instances have been configured to query an on-premise Data center DNS server. But the Instances are not able to reach the On-premise server. Which of the following could be a reason for this? Choose 2 answers from the options given below

- [ ] **A.** The Security Groups for the EC2 Instances are blocking incoming on port 53
- [ ] **B.** The NACL's are blocking outgoing on port 53 for TCP ✔
- [ ] **C.** The NACL's are blocking outgoing on port 53 for UDP ✔
- [ ] **D.** The NACL's are blocking incoming on port 53 for TCP
- [ ] **E.** The NACL's are blocking incoming on port 53 for UDP

Explanation :

Answer – B and C
In order to communicate with a DNS Server , the instance needs to reach the DNS server on port 53 for both TCP and UDP
Options A,D and E are invalid , since this issue is with the outgoing traffic
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 25 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company is planning on setting up an application that consists of EC2 Instances , an Application Load Balancer and Cloudfront. Your management is worried about DDOs attacks. Which of the following can help protect against such network attacks? Choose 3 answers from the options given below

- ☐ **A.** Place the AWS WAF in front of the Application Load Balancer ✔
- ☐ **B.** Place the AWS WAF in front of the Cloudfront Distribution ✔
- ☐ **C.** Place the AWS WAF in front of the EC2 Instances
- ☐ **D.** Consider using AWS Shield Advanced ✔

Explanation :

Answer – A,B and D
The AWS Documentation mentions the following

AWS WAF is a web application firewall that lets you monitor the HTTP and HTTPS requests that are forwarded to Amazon CloudFront or an Application Load Balancer. AWS WAF also lets you control access to your content. Based on conditions that you specify, such as the IP addresses that requests originate from or the values of query strings, CloudFront or an Application Load Balancer responds to requests either with the requested content or with an HTTP 403 status code (Forbidden).
AWS Shield Advanced provides expanded DDoS attack protection for your Amazon EC2 instances, Elastic Load Balancing load balancers, CloudFront distributions, and Route 53 hosted zones. AWS Shield Advanced incurs additional charges.
Option C is incorrect since AWS WAF can only be used with the Application Load Balancer and the Cloudfront Distribution
For more information on AWS WAF , please refer to the below URL

- https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html (https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html)

Ask our Experts

QUESTION 26 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on using Cloudfront along with S3 as the origin. There is a requirement to serve private content from S3. There is a requirement to ensure that access is restricted for certain individual files. How would you deliver the private content.

- A. Use Signed URL's ✔
- B. Use Signed Cookies
- C. Use Private Keys
- D. Use Security Groups

Explanation :

Answer – A
The AWS Documentation mentions the following
Use signed URLs in the following cases:

- You want to use an RTMP distribution. Signed cookies aren't supported for RTMP distributions.
- You want to restrict access to individual files, for example, an installation download for your application.
- Your users are using a client (for example, a custom HTTP client) that doesn't support cookies.

Use signed cookies in the following cases:

- You want to provide access to multiple restricted files, for example, all of the files for a video in HLS format or all of the files in the subscribers' area of a website.
- You don't want to change your current URLs.

Option B is incorrect since here access needs to be restricted for certain individual files
Option C is incorrect since this is better for encryption purposes
Option D is incorrect since this should be used for EC2 Instances
For more information on a better understanding on serving private content , please refer to the below URL

- https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html (https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/private-content-choosing-signed-urls-cookies.html)

Ask our Experts

QUESTION 27 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You have a set of EC2 Instances that are deployed in a VPC. An application is hosted on these instances. There are some issues which keep on recurring in the application and you plan to inspect the packets being sent from the application to trace the error. How can you achieve this?

- A. Use VPC Flow logs
- B. Use an IDS ✔
- C. Use Cloudtrail
- D. Use Cloudwatch Logs

Explanation :

Answer – B
Here you will need a custom Intrusion Detection system to do a packet level analysis.
Options A and D are incorrect since these solutions cannot do packet monitoring
Option C is incorrect since this is used to monitor API activity
For more information on IDS, please refer to the below URL

- https://aws.amazon.com/mp/scenarios/security/ids/ (https://aws.amazon.com/mp/scenarios/security/ids/)

Ask our Experts

QUESTION 28 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have a requirement to ensure that hosted zones created in Route 53 have name servers that resonate with your domain name. How can you achieve this? Choose 2 answers from the options given below

- A. Specify the domain name when creating the record set for the name servers
- B. Create a Reusable deletion set using the AWS Console
- C. Create a Reusable delegation set using Route 53 API's ✔

☐ **D.** Create a Reusable delegation set using the AWS CLI ✔

Explanation :

Answer – C and D
The AWS Documentation mentions the following
Each Amazon Route 53 hosted zone is associated with four name servers, known collectively as a delegation set. By default, the name servers have names like ns-2048.awsdns-64.com. If you want the domain name of your name servers to be the same as the domain name of your hosted zone, for example, ns1.example.com, you can configure white label name servers, also known as vanity name servers or private name servers.
To create a reusable delegation set, you can use the Route 53 API, the AWS CLI, or one of the AWS SDKs.
For more information on reusable delegation set, please refer to the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/white-label-name-servers.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/white-label-name-servers.html)

Ask our Experts

QUESTION 29 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your account is part of a parent AWS Account that has a Direct Connect connection. You plan to use the AWS Direct Connection as a hosted VIF. What would you get charged for?

○ **A.** All Data transfer in

○ **B.** All Data transfer out ✔

○ **C.** The port hours

○ **D.** The initial connection charges

Explanation :

Answer – B
You will only get charged for the data transfer out
Option A is incorrect because data transfer in is free for any AWS Direct Connect connection
Option C is incorrect because this charge will be borne by the parent AWS account
Option D is incorrect because there is no such charge
For more information on AWS Direct connect pricing, please refer to the below URL

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

Ask our Experts

QUESTION 30 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have 2 VPC's VPCA(172.16.0.0/16) and VPCB(10.0.0.0/16). You are planning on establishing VPC connecting peering. Which of the following routes need to be added to the route table for both VPC's to ensure communication across VPC's. Choose 2 answers from the options given below. Assume that the Target for the VPC Peering connection has an ID of pcx-1122

☐ **A.** In the Route table for VPCA add a route of 172.16.0.0/16 and Target as pcx-1122

☐ **B.** In the Route table for VPCA add a route of 10.0.0.0/16 and Target as pcx-1122 ✔

- [ ] **C.** In the Route table for VPCB add a route of 172.16.0.0/16 and Target as pcx-1122 ✔
- [ ] **D.** In the Route table for VPCB add a route of 10.0.0.0/16 and Target as pcx-1122

Explanation :

Answer - B and C
An example is given on the AWS documentation on this as per the snapshots below. And this also gives the Route table configurations

Two VPCs Peered Together

You have a VPC peering connection (pcx-11112222) between VPC A and VPC B, which are in the same AWS account, and do not have overlapping CIDR blocks.

The route tables for each VPC point to the relevant VPC peering connection to access the entire CIDR block of the peer VPC.

Route table	Destination	Target
VPC A	172.16.0.0/16	Local
	10.0.0.0/16	pcx-11112222
VPC B	10.0.0.0/16	Local
	172.16.0.0/16	pcx-11112222

Options A and D are incorrect because the route entry is invalid
For more information on this example , one can visit the below URL

- http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html

(http://docs.aws.amazon.com/AmazonVPC/latest/PeeringGuide/peering-configurations-full-access.html)

Ask our Experts

QUESTION 31 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You need to have instances created in a VPC which can support network speeds of upto 20 GPbs. Which of the following would be part of your implementation steps? Choose 2 answers from the options given below

- [ ] **A.** Create an Instance from an Instance type that supports the Intel 82599 VF interface
- [ ] **B.** Create an Instance from an Instance type that supports Enhanced Networking ✔
- [ ] **C.** Enable Enhanced Networking if not already done ✔
- [ ] **D.** Place the Instances in a placement group

Explanation :

Answer – B and C
For speeds for up to 25 Gbps , you need to choose an Instance type that supports Enhanced Networking
Also ensure that Enhanced Networking is enabled on the device
Option A is incorrect since this only supports a maximum of 10 Gbps
Option D is incorrect since this is only required for low latency inter Instance communication.
For more information on Enhanced Networking , one can visit 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 32 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You currently have setup a VPC and subnets in AWS. You have setup routes in the route table for traffic on the CIDR block of 0.0.0.0/0. You just want to establish communication across all hosts. But you notice that some applications are not working as desired. These are Ipv6 based applications that are sitting across subnets in the VPC. What must be done to alleviate this issue?

- **A.** Ensure that the route of 0.0.0.0/0 is removed and a more specific route is placed.
- **B.** Remove the route of 0.0.0.0/0 and add the route of ::/0 instead to allow all communication.
- **C.** Add a route for ::/0 to the route table as well. ✔
- **D.** Add the default route of 172.132.0.0/16 to the Route table

Explanation :

Answer – C
The AWS Documentation mentions the following
CIDR blocks for IPv4 and IPv6 are treated separately. For example, a route with a destination CIDR of 0.0.0.0/0 (all IPv4 addresses) does not automatically include all IPv6 addresses. You must create a route with a destination CIDR of ::/0 for all IPv6 addresses.
Options A and B are invalid since this would then stop communication for instances for

Ipv4
Option D is invalid because this CIDR block is not mentioned in the question
For more information on Route propagation , one can visit the below URL

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

Ask our Experts

QUESTION 33 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

When configuring Active Passive configuration for your VPN connections which of the following can be used to achieve such a configuration. Choose 2 answers from the options given below

- [ ] **A.** Use AS_PATH prepending ✔
- [ ] **B.** Use more specific routes ✔
- [ ] **C.** Use IPSec routing
- [ ] **D.** Use different ASN numbers

Explanation :

Answer – A and B
The AWS Documentation mentions this
multi-data-center-config
Redundant Active/Active VPN Connections
Many AWS customers choose to implement VPN connections because they can be a quick, easy, and cost-effective way to set up remote connectivity to a VPC. To enable redundancy, each AWS Virtual Private Gateway (VGW) has two VPN endpoints with capabilities for static and dynamic routing. Although statically routed VPN connections

from a single customer gateway are sufficient for establishing remote connectivity to a VPC, this is not a highly available configuration. The best practice for making VPN connections highly available is to use redundant customer gateways and dynamic routing for automatic failover between AWS and customer VPN endpoints. For simplicity, the diagram in the next section depicts each VPN connection, consisting of two IPsec tunnels to both VGW endpoints, as a single line.

Configuration Details

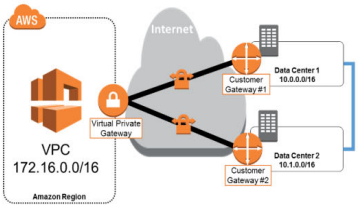
The configuration in this example consists of four fully meshed, dynamically routed IPsec tunnels between both VGW endpoints and two customer gateways. AWS provides configuration templates for a number of supported VPN devices to assist in establishing these IPsec tunnels and configuring BGP for dynamic routing. In addition to the AWS-provided VPN and BGP configuration details, customers must configure VPCs to efficiently route traffic to their data center networks. In this example, the VGW will prefer to send 10.0.0.0/16 traffic to Data Center 1 through Customer Gateway 1, and only reroute this traffic through Data Center 2 if the connection to Data Center 1 is down. Likewise, 10.1.0.0/16 traffic will prefer the VPN connection originating from Data Center 2.
AWS recommends using one of the following approaches for communicating these route preferences (For a full explanation of VPC routing rule algorithm, see Configuring Multiple VPN Connections to Your Amazon VPC):

- More specific routes: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise a summary route of 10.0.0.0/15. In addition, Customer Gateway 1 advertises 10.0.0.0/16 and Customer Gateway 2 advertises 10.1.0.0/16. AWS will use the more specific routes to send traffic to the appropriate data center, and will fail back to the other data center following the summarized route if the more specific route becomes temporarily unavailable.

- AS-path prepending: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise 10.0.0.0/16 and 10.1.0.0/16. However, Customer Gateway 1 uses AS-path prepending when advertising the 10.1.0.0/16 network to make this route less preferred. Likewise, Customer Gateway 2 uses AS-path prepending when advertising the 10.0.0.0/16 network to make this route less preferred. AWS will use the preferred routes to send traffic to the appropriate data center, and will fail back to the other data center following the less preferred routes when necessary.

Configuration Details

The configuration in this example consists of four fully meshed, dynamically routed IPsec tunnels between both VGW endpoints and two customer gateways. AWS provides configuration templates for a number of supported VPN devices to assist in establishing these IPsec tunnels and configuring BGP for dynamic routing. In addition to the AWS-provided VPN and BGP configuration details, customers must configure VPCs to efficiently route traffic to their data center networks. In this example, the VGW will prefer to send 10.0.0.0/16 traffic to Data Center 1 through Customer Gateway 1, and only reroute this traffic through Data Center 2 if the connection to Data Center 1 is down. Likewise, 10.1.0.0/16 traffic will prefer the VPN connection originating from Data Center 2.



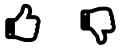
AWS recommends using one of the following approaches for communicating these route preferences (For a full explanation of VPC routing rule algorithm, see Configuring Multiple VPN Connections to Your Amazon VPC):

- More specific routes: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise a summary route of 10.0.0.0/15. In addition, Customer Gateway 1 advertises 10.0.0.0/16 and Customer Gateway 2 advertises 10.1.0.0/16. AWS will use the more specific routes to send traffic to the appropriate data center, and will fail back to the other data center following the summarized route if the more specific route becomes temporarily unavailable.
- AS-path prepending: With this approach, both Customer Gateway 1 and Customer Gateway 2 advertise 10.0.0.0/16 and 10.1.0.0/16. However, Customer Gateway 1 uses AS-path prepending when advertising the 10.1.0.0/16 network to make this route less preferred. Likewise, Customer Gateway 2 uses AS-path prepending when advertising the 10.0.0.0/16 network to make this route less preferred. AWS will use the preferred routes to send traffic to the appropriate data center, and will fail back to the other data center following the less preferred routes when necessary.

Option C is incorrect because IPSec is default used as the protocol for communication
Option D is incorrect because this would not help in this configuration
For more information on High Availability Network connections , one can 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 34 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

You have two Direct Connect connections and two VPN connections to your network.

Following are the details

Site A is VPN 10.2.0.0/24 AS 65000 65000

Site B is VPN 10.2.0.252/30 AS 65000

Site C is DX 10.0.0.0/8 AS 65000 65000

Site D is DX 10.0.0.0/16 AS 65000 65000 65000.

Which site will AWS choose to reach your network?

- A. Site A
- B. Site B ✔
- C. Site C
- D. Site D

Explanation :

Answer – B
The first order of preference is that the route will the lowest prefix will always win. Hence Site B will be chosen by AWS.
Hence all other options by default become invalid.
For more information on Route tables , one can visit 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 35 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

You've setup VPC Flow logs for your EC2 Instance ENI in a subnet. You can see the below REJECT record in the VPC Flow logs. What does this indicate.

2 123456789911 eni-abc123de 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK

- A. A request was made on port 80 to the Instance
- B. Someone was trying to log into the Instance via SSH
- C. Someone was trying to log into the Instance via RDP ✔
- D. A request was made on port 443 to the Instance

Explanation :

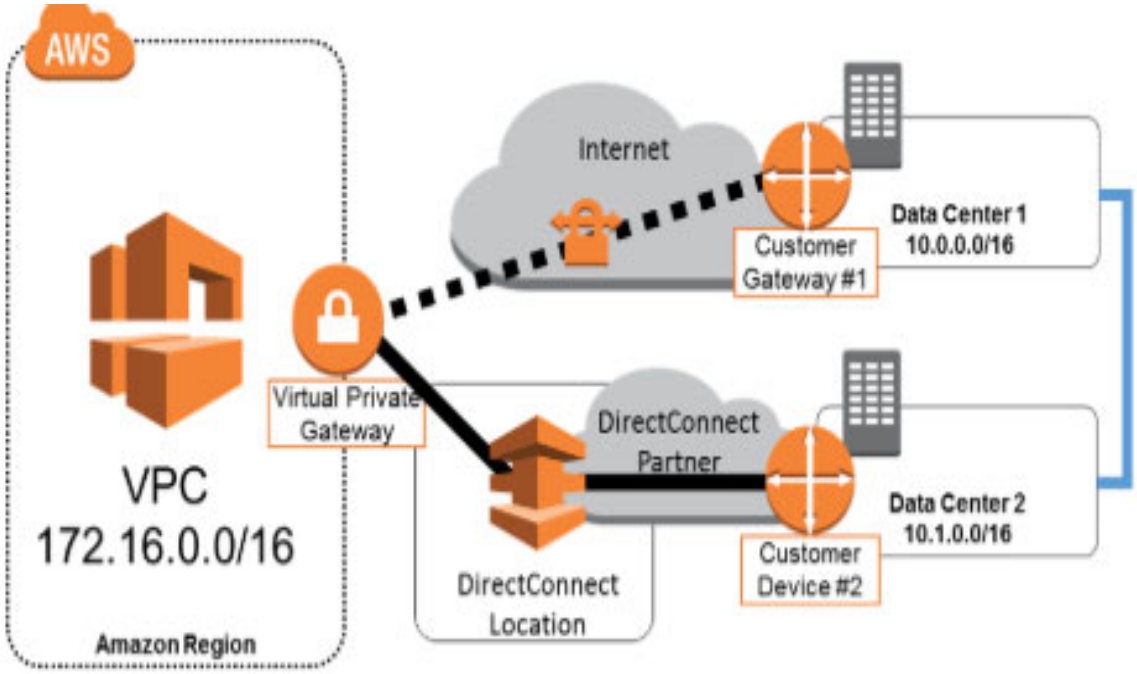
Answer – C
In the record which is recorded in VPC Flow logs , the highlighted field shown below shows that a request was made to port 3389 which is the RDP protocol
2 123456789911 eni-abc123de 172.31.9.69 172.31.9.12 49761 3389 6 20 4249 1418530010 1418530070 REJECT OK
By default all other options becomes invalid since clearly the log shows what is the port number recorded.
For more information on VPC Flow Logs , one can visit 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 36 UNATTEMPTED
DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has the following setup



The routes advertised by both Customer gateway 1 and Customer Device 2 is 10.0.0.0/15. How will the traffic flow from the data center to AWS?

- A. The traffic will flow primarily through Customer gateway 1
- B. The traffic will flow primarily through Customer device 2 ✔
- C. The traffic will flow primarily through the Internet
- D. Traffic will not flow due to the conflict in routes

Explanation :

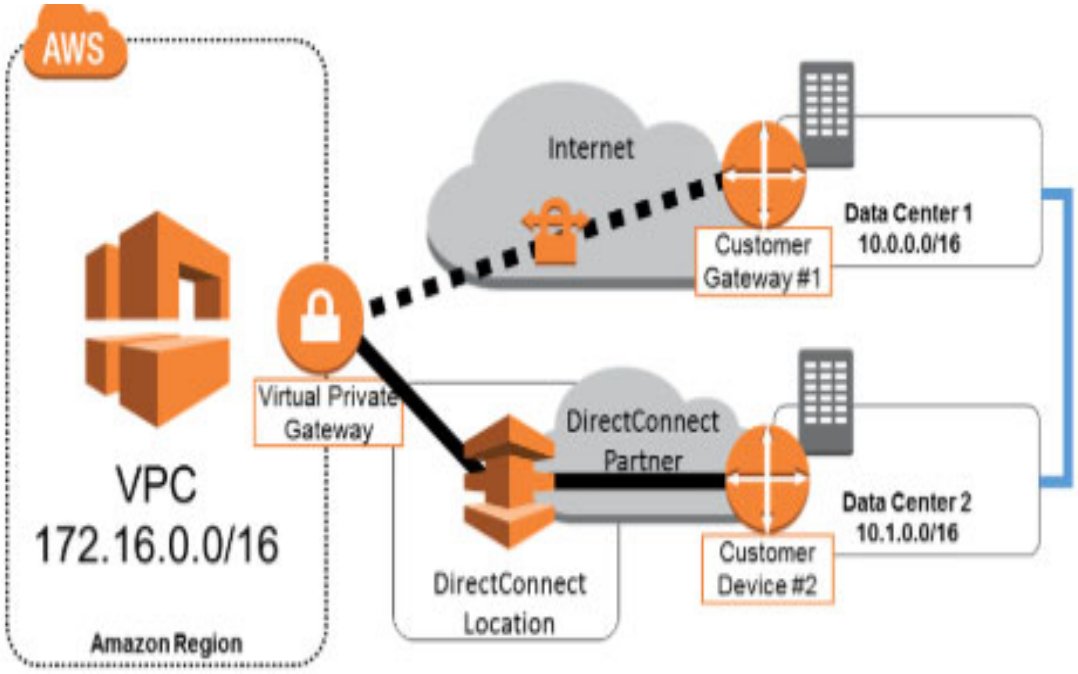
Answer – B

This sort of scenario is given in the AWS Documentation

Configuration Details

The configuration in this example consists of two dynamically routed connections, one using AWS Direct Connect and the other using a VPN connection from two different customer devices. AWS provides example router configurations to assist in establishing both AWS Direct Connect and VPN connections with BGP for dynamic routing. By default, AWS will always prefer to send traffic over an AWS Direct Connect connection, so no additional configuration is required to define primary and backup connections. In this

example, both Customer Gateway 1 and Customer Device 2 advertise a summary route of 10.0.0.0/15 and AWS will send all traffic to Customer Device 2 as long as this network path is available.



By default all other options become invalid

For more information on Data Center High Availability, one can 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 37 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You've setup a VPN connection between your on-premise data center and AWS. You need to know how the VPN connection will cost. Which of the below is a factor to be considered when looking at the costing for VPN connections.

- A. DataTransfer In
- B. DataTransfer Out
- C. Virtual Private Gateway transfer out
- D. VPN connection hours ✔

Explanation :

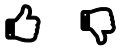
Answer – D
By default all other options become invalid
This is given in the AWS Documentationextension of your corporate datacenter.
VPN Connection Pricing

- $0.05 per VPN Connection-hour
- $0.048 per VPN Connection-hour for connections to the Tokyo Region and Osaka-Local Region
- $0.065 per VPN Connection-hour for AWS GovCloud (US) Region

If you choose to create a VPN Connection to your VPC using a Virtual Private Gateway, you are charged for each "VPN Connection-hour" that your VPN connection is provisioned and available. Each partial VPN Connection-hour consumed is billed as a full hour. You also incur standard AWS data transfer charges for all data transferred via the VPN Connection. If you no longer wish to be charged for a VPN Connection, you simply terminate your VPN Connection using the AWS Management Console, command line interface, or API.
For more information on the pricing, one can visit the below URL

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

Ask our Experts



QUESTION 38 UNATTEMPTED AUTOMATE AWS TASKS

Your company currently uses NAT instances to route traffic for Instances in private subnets. They need to convert these to NAT gateways to increase the amount of bandwidth required. They want to automate the provision. How can you accomplish this?

- **A.** Use AWS Config to change the configuration of the NAT instance to a NAT gateway
- **B.** Use Cloudformation templates to replace the NAT instances with NAT gateways ✔
- **C.** Use Opswork to replace the NAT instances with NAT gateways
- **D.** Use AWS Inspector to replace the NAT instances with NAT gateways

Explanation :

Answer – B
This example is also given in the AWS Documentation
Modifying your CloudFormation template to discontinue the use of NAT instances and consume NAT gateways is straightforward. You would:

- Allocate an Elastic IP address. However, it would not be directly assigned to an instance.
- Create a NAT gateway resource.
- Create a route to the Internet, but via the NAT gateway instead of going through a NAT instance. As in the code for NAT instances, this route would then be associated with the route table for the private subnets in the same Availability Zone.

The updated example would look something like this:

```
{
  ...
  "Resources" : {
    ...
    "NATGateway1EIP" : {
      "Type" : "AWS::EC2::EIP",
      "Properties" : {
        "Domain" : "vpc"
      }
    },
    "NATGateway1" : {
```

```
      "Type" : "AWS::EC2::NatGateway",
      "DependsOn" : "VPCGatewayAttachment",
      "Properties" : {
        "AllocationId" : {
          "Fn::GetAtt" : [
            "NATGateway1EIP",
            "AllocationId"
          ]
        },
        "SubnetId" : {
          "Ref" : "PublicSubnetAZ1"
        }
      }
    },
    "PrivateRoute1" : {
      "Type" : "AWS::EC2::Route",
      "Properties" : {
        "RouteTableId" : {
          "Ref" : "PrivateRouteTable1"
        },
        "DestinationCidrBlock" : "0.0.0.0/0",
        "NatGatewayId" : {
          "Ref" : "NATGateway1"
        }
      }
    },
    ...
  }
  ...
}
```

Option A is invalid because AWS Config can only check for the configuration of resources
Option C is invalid because this is used to create stacks of resources and in this case It is better to use Cloudformation
Option D is invalid because AWS Inspector is used to scan for the vulnerability of Instances
For more information on the using cloudformation templates for NAT gateways , one can visit the below URL

- https://aws.amazon.com/blogs/apn/taking-nat-to-the-next-level-in-aws-cloudformation-templates/ (https://aws.amazon.com/blogs/apn/taking-nat-to-the-next-level-in-aws-cloudformation-templates/)

Ask our Experts

QUESTION 39 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

When configuring a Public VIF for AWS Direct Connect , which of the following is not required in the configuration

- A. VLAN ID
- B. Router Peer IP
- C. BGP ASN
- D. Virtual Private Gateway ✔

Explanation :

Answer-D
Options A,B and C are incorrect since all of these are required when creating a Public VIF
The Virtual Private Gateway is only required when you are crating a Private VIF
Below is the screenshot of what is required when creating a Private VIF

For more information on creating a public VIF , one can visit 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 40 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company currently has VPC's located in us-west and us-east. The company has an AWS Direct Connect connection in the US East region. They want to have the ability to extend the connection to us-west. They also need to minimize time and effort to have this in place. How can this be achieved?

- A. Create another AWS Direct Connect connection in us-west
- B. Make use of the Direct Connect gateway ✔
- C. Create a private VIF using the current connection
- D. Make use of an IPSec VPN

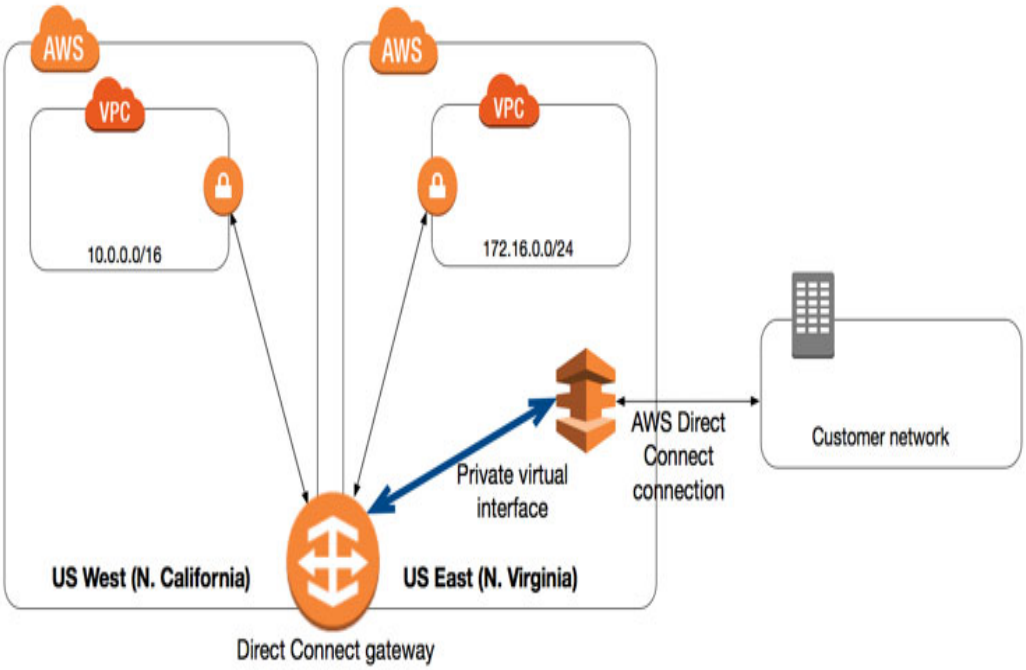
Explanation :

Answer – B

The AWS Documentation mentions the following

You can use an *AWS Direct Connect gateway* to connect your AWS Direct Connect connection over a private virtual interface to one or more VPCs in your account that are located in the same or different regions. You associate a Direct Connect gateway with the virtual private gateway for the VPC, and then create a private virtual interface for your AWS Direct Connect connection to the Direct Connect gateway. You can attach multiple private virtual interfaces to your Direct Connect gateway.

The below diagram from the AWS Documentation shows how this can be achieved.



Option A is incorrect since creating another connection would just be an overhead

Option C is incorrect since this could only extend to the current region
Option D is incorrect since there is no mention of encryption required
For more information on the Direct Connect gateway , one can visit the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways.html)

Ask our Experts

QUESTION 41 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your company has setup an application load balancer and various targets behind the ALB. But there are continuous problems at times wherein clients cannot connect to the ALB , because of the whitelisting that is required to be done by the IT Security department. What changes can be made to the architecture to alleviate this problem.

- A. Assign a public IP to the Application Load Balancer
- B. Assign an Elastic IP to the Application Load Balancer
- C. Place a Network Load balancer in front of the ALB ✔
- D. Place a Network Load balancer behind the ALB

Explanation :

Answer – C
Since the IP of the Application Load balancer keeps on changing , the workaround is to have a Network Load balancer in front of the ALB. An elastic IP is then assigned to the Network Load balancer and in this way the IP address wont change.
Options A and B are incorrect because you can't assign IP addresses to Application Load Balancers
Option D is incorrect because it needs to be the other way around
For more information on this scenario , one can visit the below URL

- https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/ (https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/)

Ask our Experts

QUESTION 42 UNATTEMPTED

CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have a Cloudfront distribution that has an S3 bucket as the origin. There is a requirement to add Security headers to the response before it can be relayed back to the user. How can you achieve this?

- A. Change the Behaviour of the origin. Add a configuration for adding the security header.
- B. Create a Lambda function that will run on the edge ✔
- C. Make sure that the Viewer protocol is set to HTTPS
- D. Create an OAI for the Cloudfront distribution

Explanation :

Answer – B
One of the AWS Blogs mentions the following
Lambda@Edge provides the ability to execute a Lambda function at an Amazon CloudFront Edge Location. This capability enables intelligent processing of HTTP requests at locations that are close (for the purposes of latency) to your customers. To get started, you simply upload your code (Lambda function written in Node.js (https://nodejs.org/en/)) and pick one of the CloudFront behaviors associated with your distribution.
All other options are incorrect since none of these will help meet the requirement
For more information on adding security headers using Lambda@Edge , one can visit the below URL

- https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/ (https://aws.amazon.com/blogs/networking-and-content-delivery/adding-http-security-headers-using-lambdaedge-and-amazon-cloudfront/)

Ask our Experts

QUESTION 43 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

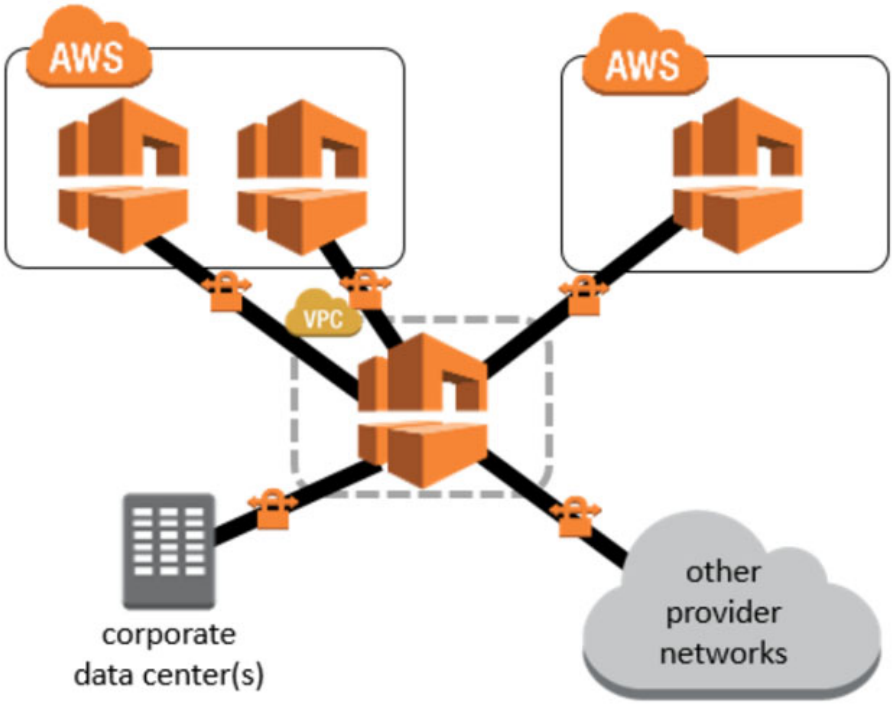
Your company has setup a VPN connection between their on-premise infrastructure and AWS. They have multiple VPC's defined. They also need to ensure that all traffic flows through a security VPC from their on-premise infrastructure. How would you architect the solution? Choose 2 answers from the options given below

- [ ] **A.** Create a VPN connection between the On-premise environment and the Security VPC ✔
- [ ] **B.** Create a VPN connection between the On-premise environment to all other VPC's
- [ ] **C.** Create a VPN connection between the Security VPC to all other VPC's ✔
- [ ] **D.** Create a VPC peering connection between the Security VPC and all other VPC's

Explanation :

Answer – A and C

This is a design which incorporates a transit VPC. The below diagram from the AWS documentation demonstrates this



Option B is incorrect since this would go against the concept of the Transit VPC
Option D is incorrect since transitive routing is not possible across peering connections from a VPN connection
For more information on the transit VPC , one can visit the below URL

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/transit-vpc.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/transit-vpc.html)

Ask our Experts

QUESTION 44 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on testing out Amazon workspaces for their account. They are going to allocate a set of workstations with static IP addresses for this purpose. They need to ensure that only these IP addresses have access to Amazon Workspaces. How can you achieve this?

- A. Create an IP access control group ✔
- B. Place a WAF in front of Amazon Workspaces
- C. Specify the IP addresses in the NACL
- D. Specify the IP addresses in the Security Group

Explanation :

Answer – A
The AWS Documentation mentions the following
An IP access control group acts as a virtual firewall that controls the IP addresses from which users are allowed to access their WorkSpaces. You can associate each IP access control group with one or more directories. You can associate up to 25 IP access control groups with each directory.
Option B is incorrect because a WAF can only be placed in front of an Application Load balancer or a Cloudfront distribution
Options C and D are incorrect since these are used for traffic control to subnets and EC2 Instances
For more information on restricting access , one can visit the below URL

- https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html (https://docs.aws.amazon.com/workspaces/latest/adminguide/amazon-workspaces-ip-access-control-groups.html)

Ask our Experts

QUESTION 45 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have a RESTful service that is developed by your company. You want to provide secure access to this service to multiple clients. The service is hosted in a private subnet in one of your VPC's. How can you accomplish this?

- A. Create a VPC Endpoint gateway for your service
- B. Create a VPC Interface Endpoint ✔
- C. Create an application load balancer and provide the DNS name to your clients
- D. Create a network load balancer and provide the DNS name to your clients

Explanation :

Answer – B
The AWS Documentation mentions the following
An interface VPC endpoint (AWS PrivateLink) enables you to connect to services powered by AWS PrivateLink. These services include some AWS services, services hosted by other AWS accounts (referred to as *endpoint services*), and supported AWS Marketplace partner services. The interface endpoints are created directly inside of your VPC, using elastic network interfaces and IP addresses in your VPC's subnets. The service is now in your VPC, enabling connectivity to AWS services or AWS PrivateLink-powered service via private IP addresses. That means that VPC Security Groups can be used to manage access to the endpoints. Also, interface endpoint can be accessed from your premises via AWS Direct Connect.
Option A is incorrect since this is used for public services such as S3 and DynamoDB
Options C and D are incorrect since the services are located in the private subnet , so the DNS name would not be available to users on the Internet
For more information on AWS private link , one can visit the below URL

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-privatelink.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/aws-privatelink.html)

Ask our Experts

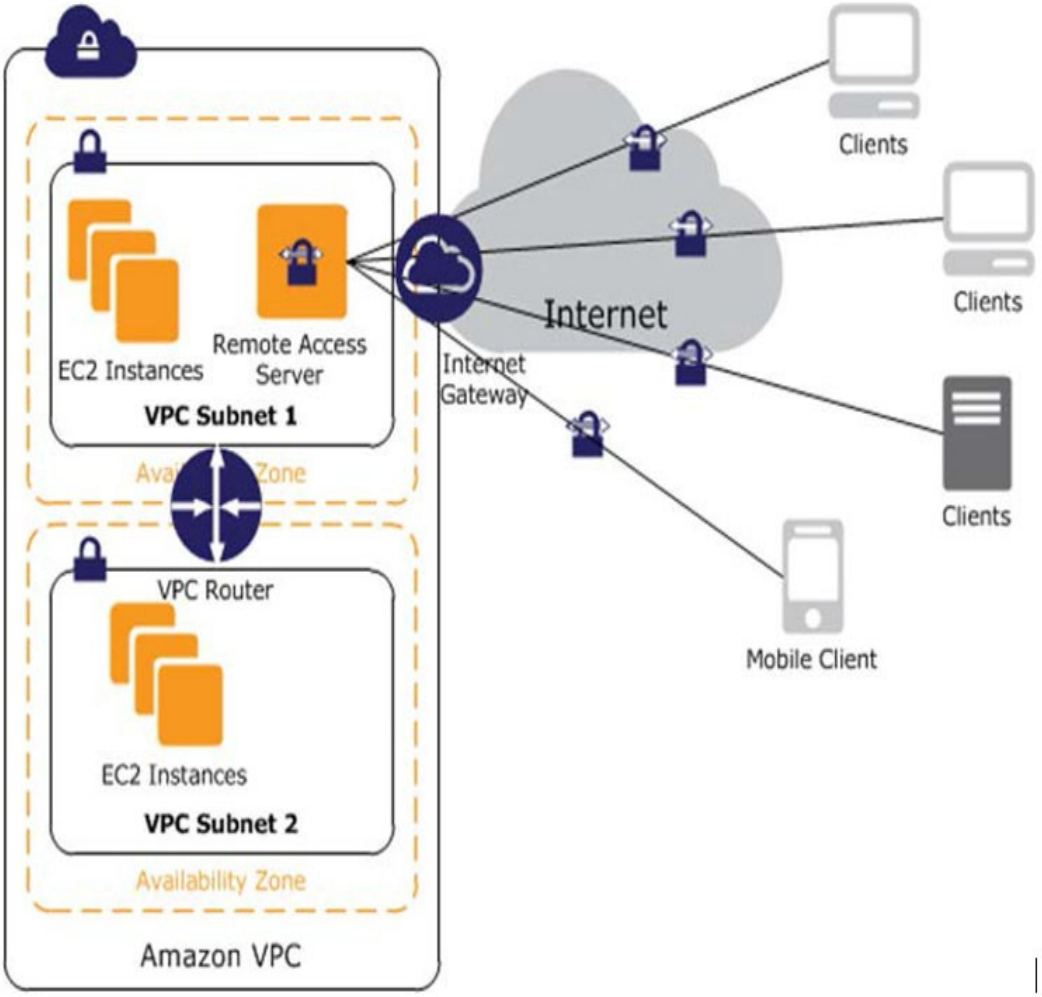
QUESTION 46 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have a requirement of providing remote access to clients from their mobile devices and tablets. This is to access a service from inside a VPC. Which of the following would be part of the design?

- **A.** A custom VPN server hosted on an EC2 Instance ✔
- **B.** An AWS Managed VPN
- **C.** An AWS Managed Direct Connect connection
- **D.** An AWS Managed Direct Connect gateway

Explanation :

Answer – A
To connect single clients, you need to have a custom VPN server. The below diagram from the AWS Documentation shows how this can be achieved.



Options B,C and D are incorrect since these are used to connect site locations to AWS
For more information on Remote Access connectivity , one can visit the below URL

- https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-remote-access-vpn-internal-user.html (https://docs.aws.amazon.com/aws-technical-content/latest/aws-vpc-connectivity-options/software-remote-access-vpn-internal-user.html)

Ask our Experts

QUESTION 47 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company has setup an AWS Direct Connect connection along with a public VIF. There is a concern raised by the IT security department regarding the loopholes with a public VIF. Which of the following is a valid concern that could be raised by the security department?

- **A.** An EC2 Instance with a public IP has a chance of reaching you via the public VIF ✔
- **B.** An EC2 Instance with a private IP has a chance of reaching you via the public VIF
- **C.** Your VPC gets exposed to the Internet
- **D.** Your VPC gets exposed via the public VIF

Explanation :

Answer – A
This is provided in one of the Re-invent talks where , the public IP's get advertised and is reachable via the public VIF

All other options are wrong since it's only the public IP's that get advertised

For more information on the Reinvent video , one can visit the below URL

- https://www.youtube.com/watch?v=eNxPhHTN8gY (https://www.youtube.com/watch?v=eNxPhHTN8gY)

Ask our Experts

QUESTION 48 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Which of the following can be used to control how far your routes gets advertised when using AWS Direct Connect and a public VIF.

- **A.** Use BGP communities ✔
- **B.** Use BGP headers
- **C.** Use AS_PATH prepending
- **D.** Use MED

Explanation :

Answer – A
This is also mentioned in the AWS Documentation
BGP Communities
AWS Direct Connect supports a range of BGP community tags to help control the scope (regional or global) and route preference of traffic.
Scope BGP Communities
You can apply BGP community tags on the public prefixes you advertise to Amazon to indicate how far to propagate your prefixes in the Amazon network—for the local AWS Region only, all regions within a continent, or all public regions.
You can use the following BGP communities for your prefixes:

- 7224:9100—Local AWS Region
- 7224:9200—All AWS regions for a continent (for example, North America–wide)
- 7224:9300—Global (all public AWS Regions)

All other options are invalid since you need to use BGP communities
For more information on routing and BGP communities , one can visit the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html (https://docs.aws.amazon.com/directconnect/latest/UserGuide/routing-and-bgp.html)

Ask our Experts

QUESTION 49 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is using a hosted virtual interface from its parent AWS Account. You need to mention to IT management on what charges your company will acquire. Which of the following would you mention?

- A. The port hour charges
- B. The data transfer in
- C. The data transfer out via the interface ✔
- D. The amount of hours used by the interface

Explanation :

Answer – C
The AWS Documentation currently mentions the following
Data Transfer via AWS Direct Connect will be billed in the same month in which the usage occurred. If you have a hosted virtual interface, you will only be charged for the data transferred out of that virtual interface at the applicable Data Transfer rates. The account that owns the port will be charged the port-hour charges
All other options are invalid since it is clearly mentioned what you get charged for in the AWS Documentation
For more information on Direct Connect , one can visit the below URL

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

Ask our Experts

QUESTION 50 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You're working as a consultant for a company that has a three-tier application. The application layer of this architecture sends over 20Gbps of data per seconds during peak hours to and from Amazon S3. Currently, you're running two NAT gateways in two subnets to transfer the data from your private application layer to Amazon S3. You will also need to ensure that the instances receive software patches from a third-party repository. What architecture changes should be made, if any?

- A. Add another NAT gateway
- B. Add a VPC endpoint. ✔
- C. Add an Internet gateway for better throughput
- D. Add a VPN connection for better throughput

Explanation :

Answer – B
The AWS Documentation mentions the following
A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.
Option A is incorrect since the 2 NAT gateways are sufficient. The NAT gateway can scale up to 45 Gbps
Option C is incorrect since the subnet needs to remain private
Option D is incorrect because the bandwidth can degrade due to a VPN connection
For more information on VPC endpoints , one can visit the below URL

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

Ask our Experts

QUESTION 51 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

Your on-premise network has an IP address range of 152.55.0.0/16. You have been allocated an address range of 152.55.253.0/24 for the AWS Cloud. You need to design the VPC and ensure communication between the VPC and your on-premise network. How would you accomplish this. Choose 2 answers from the options given below

- [ ] **A.** Setup a VPC with an address range of 152.55.0.0/16
- [ ] **B.** Setup a VPC with an address range of 152.55.253.0/24 ✔
- [ ] **C.** Establish a VPN connection using your customer gateway. Ensure a route is present in youron-premise router to route traffic via the customer gateway. ✔
- [ ] **D.** Establish a VPN connection using your virtual private gateway. Ensure a route is present in your on-premise router to route traffic via the virtual private gateway.

Explanation :

Answer - B and C
Since the Address range assigned for the cloud is 152.55.253.0/24. This should be the address range assigned to the VPC
Then use the customer gateway on your side to route traffic through the VPN tunnel
Option A is incorrect since this is not the IP range assigned for the AWS Cloud
Option D is incorrect since the virtual private gateway is assigned to the VPC and not on the on-premise network
For more information on setting up a VPN connection, one can visit the below URL

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

Ask our Experts

QUESTION 52 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You've setup a VPC with a couple of Instances that have public IP addresses. These EC2 Instances need to reach an external web server on port 443. The instances are unable to reach the web server. You have verified the following

- An internet gateway is assigned to the VPC(10.0.0.0/16)
- The route table has a route for 0.0.0.0/0 to the Internet gateway
- The Security Groups allows Outbound Traffic for port 443
- The NACL allows Outbound Traffic for port 443 and Inbound Traffic for ephemeral ports

Based on the above information what could be the underlying issue.

- **A.** You should not use the Internet gateway , instead use a NAT gateway for the routing of traffic
- **B.** The route table should have a route for 10.0.0.0/16 to the Internet gateway
- **C.** The Security Group should allow Inbound traffic for port 443
- **D.** The external web server is blocking the requests ✔

Explanation :

Answer – D
All of the settings are right for ensuring traffic can reach the external web server. In the end the issue could be at the web server end and it is blocking traffic
Option A is incorrect since NAT gateways should be used for Instances in private subnets
Option B is incorrect since the route table is already correct
Option C is incorrect since the Security Groups settings are correct
For more information on Amazon VPC, one can visit the below URL

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

Ask our Experts

QUESTION 53 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on setting up an AWS Direct Connect connection. Which of the following is not required for setting up the connection?

- A. Support for the router for IPSec ✔
- B. Support for the router for BGP
- C. Single mode fiber
- D. VLAN encapsulation

Explanation :

Answer – A
Below are the requirements for AWS Direct Connect
· 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.

All other options are invalid because these are all key requirements for AWS Direct Connect

For more information on AWS Direct Connect, one can visit the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf (https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf)

Ask our Experts

QUESTION 54 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Your company is planning on using a Sub 1Gbps hosted connection. What are the steps that need to be carried out before you can start creating a virtual interface using this connection?

- **A.** Create the hosted connection in the console
- **B.** Request for an AWS Direct Connect connection via AWS Support
- **C.** Accept the hosted connection in the console ✔
- **D.** Raise a support ticket to accept the hosted connection

Explanation :

Answer – C

This is mentioned in the AWS Documentation

If you requested a sub-1G connection from your selected partner, they create a hosted connection for you (you cannot create it yourself). You must accept it in the AWS Direct Connect console before you can create a virtual interface.
All other options are incorrect since it is clearly mentioned in the AWS Documentation how the hosted connection should be accepted.
For more information on AWS Direct Connect, one can visit the below URL

- https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf (https://docs.aws.amazon.com/directconnect/latest/UserGuide/dc-ug.pdf)

Ask our Experts

QUESTION 55 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

You have an EC2 Instance that is located in a subnet mapped to an Availability zone. Due to a recent network redesign by your network architects the Instance needs to be moved to another subnet which is mapped to the same availability zone. How can you achieve this?

- **A.** Create an AMI out of the EC2 Instance. Launch a new Instance out of the AMI in the new subnet. ✔
- **B.** Create an ENI in the new subnet. Attach it to the Instance
- **C.** Assign a new private IP address which pertains to the new subnet and then assign it to the Instance
- **D.** Assign a new public IP address which pertains to the new subnet and then assign it to the Instance

Explanation :

Answer – A
This is also given in the AWS Documentation
How do I move my EC2 instance to another subnet, Availability Zone, or VPC?
Issue

I want to move or copy my EC2 instance to another subnet, Availability Zone, or VPC. How do I do that?

Short Description

To move an EC2 instance, create a new Amazon Machine Image (AMI) in the desired target Availability Zone, launch a new instance based on this image, and then reassign the Elastic IP address from the instance you are moving to the new image.

Note: This procedure is the same for copying or moving an instance between subnets, even if they are in the same Availability Zone.

All other options automatically become invalid because of this restriction

For more information on moving EC2 Instances, one can visit the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/ (https://aws.amazon.com/premiumsupport/knowledge-center/move-ec2-instance/)

Ask our Experts

QUESTION 56 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company has a set of EC2 Instances defined in a VPC. They need to monitor the traffic flowing into the Instances. They also need to monitor all the API calls occurring on the EC2 Instances. Which of the following services can help fulfil this requirement?

- A. Amazon CloudWatch Logs and VPC Flow Logs
- B. AWS CloudTrail and VPC Flow Logs ✔
- C. AWS CloudTrail and CloudWatch Logs
- D. AWS CloudTrail and AWS Config

Explanation :

Answer – B
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.
AWS CloudTrail is an AWS service that helps you enable governance, compliance, and operational and risk auditing of your AWS account. Actions taken by a user, role, or an AWS service are recorded as events in CloudTrail. Events include actions taken in the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.
Options A and C is invalid since CloudWatch Logs cannot capture traffic or API calls
Option D is invalid because AWS Config cannot capture traffic
For more information on VPC Flow logs, one can visit 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)

For more information on Cloudtrail, one can visit the below URL

- https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html (https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)

Ask our Experts

QUESTION 57 UNATTEMPTED

DESIGN AND IMPLEMENT HYBRID IT NETWORK ARCHITECTURES AT SCALE

Your company currently has a VPC and an AWS Direct connect connection to AWS. They need to move data between the on-premise location and the VPC in the most secure manner possible. You need to ensure confidentiality and integrity of the data in transit to your VPC. Which 3 steps would you take to accomplish this.

- [ ] **A.** Setup a private VIF using the AWS Direct Connect connection
- [ ] **B.** Setup a public VIF using the AWS Direct Connect connection ✔
- [ ] **C.** Attach a virtual private gateway to the VPC ✔
- [ ] **D.** Create a IPSec tunnel between the customer gateway and the virtual private gateway ✔

Explanation :

Answer – B,C and D
This is also given in the AWS Documentation
Short Description
A VPN that connects your office to your Amazon VPC over an AWS Direct Connect connection is likely to be faster and more secure than a VPN that connects to your VPC over the internet.
Resolution

1. Create an AWS Direct Connect connection.
2. Configure a public virtual interface for the Direct Connect connection.
3. In the Prefixes you want to advertise field for the virtual interface, enter the IPv4 CIDR destination addresses (separated by commas) where traffic should be routed to you over the virtual interface. In this case, add the customer gateway (VPN device) public IP, as well as any network prefixes that you want to advertise.

Note: The customer gateway (VPN device) can be configured in a Border Gateway Protocol (BGP) ASN.
Your public virtual interface receives all the public IP addresses from AWS regions (except the AWS China region), including the public IP addresses of the VPN. To get the current list of prefixes advertised by AWS, download the JSON file containing AWS IP address ranges. For more information, see AWS IP Address Ranges.
Option A is incorrect since you cannot enable IPsec over the private connection
For more information on VPN over Direct Connect, one can visit the below URL

- https://aws.amazon.com/premiumsupport/knowledge-center/create-vpn-direct-connect/ (https://aws.amazon.com/premiumsupport/knowledge-center/create-vpn-direct-connect/)

Ask our Experts

QUESTION 58 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You've configured a classic load balancer with EC2 Instances behind them. You are going to the DNS name for the load balancer , but you are not getting the response from the underlying instances. Which of the following are checks you should carry out? Choose 2 answers from the options given below

- [ ] **A.** Ensure the load balancer is created in the public subnet ✔
- [ ] **B.** Ensure the load balancer is created in the private subnet
- [ ] **C.** Ensure the Security group for the load balancer accepts traffic on port 80 from10.0.0.0/16
- [ ] **D.** Ensure the Security group for the load balancer accepts traffic on port 80 from0.0.0.0/0 ✔

Explanation :

Answer – A and D

These checks are also given in the AWS Documentation

Troubleshoot a Classic Load Balancer: Client Connectivity

If your Internet-facing load balancer in a VPC is not responding to requests, check for the following:

Your Internet-facing load balancer is attached to a private subnet

Verify that you specified public subnets for your load balancer. A public subnet has a route to the Internet Gateway for your virtual private cloud (VPC).

A security group or network ACL does not allow traffic

The security group for the load balancer and any network ACLs for the load balancer subnets must allow inbound traffic from the clients and outbound traffic to the clients on the listener ports. For more information, see Security Groups for Load Balancers in a VPC.

Option B is incorrect since the load balancer needs to be created in the public subnet

Option C is incorrect since the traffic needs to be allowed from anywhere

For more information on troubleshooting the load balancer, one can visit the below URL

- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-connection-failed.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/ts-elb-connection-failed.html)
- https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-troubleshooting.html (https://docs.aws.amazon.com/elasticloadbalancing/latest/classic/elb-troubleshooting.html)

Ask our Experts

QUESTION 59 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

You're trying to do some housekeeping and delete some unwanted interface. You try to delete an interface manually that has the following information

{

"Status": "in-use",

...

"Description": "VPC Endpoint Interface vpce-08233123488812123",

"NetworkInterfaceId": "eni-c8fbc27e",

"VpcId": "vpc-1a2b3c4d",

"PrivateIpAddresses": [

```
      {
        "PrivateDnsName": "ip-20-0-2-227.ec2.internal",
        "Primary": true,
        "PrivateIpAddress": "20.0.2.227"
      }
    ],
    "RequesterManaged": true,
    ...
  }
```


But you are not able to delete the interface. What is the reason as to why you cannot delete the interface?

- **A.** It's because it is a requester managed interface ✔
- **B.** It's because it has a private DNS name attached
- **C.** It's because it has a private IP address attached
- **D.** It's because its attached to a VPC

Explanation :

Answer – A
The AWS Documentation mentions the following
A requester-managed network interface is a network interface that an AWS service creates in your VPC. This network interface can represent an instance for another service, such as an Amazon RDS instance, or it can enable you to access another service or resource, such as an AWS PrivateLink service, or an Amazon ECS task.

You cannot modify or detach a requester-managed network interface. If you delete the resource that the network interface represents, the AWS service detaches and deletes the network interface for you
Options B,C and D are invalid because it's not because of these attributes as to why the network interface can't be deleted
For more information on requester managed interfaces, one can visit the below URL

- https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/requester-managed-eni.html (https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/requester-managed-eni.html)

Ask our Experts

QUESTION 60 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

An EC2 Instance has been setup in AWS. A software was successfully downloaded and installed on the EC2 Instance. This software uses IPv6 for communication. After the software was installed , and you were trying to access the software via IPv6 on port 80, you were not able to do so. What needs to be done to alleviate this issue?

- **A.** Add an inbound rule to your security group that allows inbound traffic on port 80 for ::/0. ✔
- **B.** Add an internet gateway for the instance.
- **C.** Add an inbound rule to your security group that allows inbound traffic on port 80 for 0.0.0.0/0.
- **D.** Add an egress-only internet gateway.

Explanation :

Answer – A
Since the application works on IPv6, you need to ensure that the port is open for all Ipv6 addresses as ::/0
Options B and C are incorrect since the instance can already download updates that means there is a connection to the internet and the rules for IPv4 is in place.
Option D is invalid since there is no restriction mentioned in the question for IPv6
For more information on security groups, one can visit the below URL

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

Ask our Experts

QUESTION 61 UNATTEMPTED
CONFIGURE NETWORK INTEGRATION WITH APPLICATION SERVICES

You have a collection of assets stored in an S3 bucket. You want to enable users across the world to access these assets with the least latency. The users must also access the distribution via your company domain name. How can you achieve this? Choose 2 answers from the options given below.

- [ ] **A.** Create a web based distribution in Cloudfront ✔
- [ ] **B.** Create an application load balancer and point it to your S3 bucket
- [ ] **C.** Create a resource record in a hosted zone and create an ALIAS record ✔
- [ ] **D.** Create a resource record in a hosted zone and create a PTR record

Explanation :

Answer – A and C
This is also given in the AWS Documentation

Routing Traffic to an Amazon CloudFront Web Distribution by Using Your Domain Name

If you want to speed up delivery of your web content, you can use Amazon CloudFront, the AWS content delivery network (CDN). CloudFront can deliver your entire website—including dynamic, static, streaming, and interactive content—by using a global network of edge locations. Requests for your content are automatically routed to the edge location that gives your users the lowest latency.

Note

You can route traffic to a CloudFront distribution only for public hosted zones.

To use CloudFront to distribute your content, you create a web distribution and specify settings such as the Amazon S3 bucket or HTTP server that you want CloudFront to get your content from, whether you want only selected users to have access to your content, and whether you want to require users to use HTTPS.

When you create a web distribution, CloudFront assigns a domain name to the distribution, such as d111111abcdef8.cloudfront.net. You can use this domain name in the URLs for your content, for example:

http://d111111abcdef8.cloudfront.net/logo.jpg

Alternatively, you might prefer to use your own domain name in URLs, for example:

http://example.com/logo.jpg

If you want to use your own domain name, use Amazon Route 53 to create an alias record that points to your CloudFront distribution. An alias record is a Route 53 extension to DNS. It's similar to a CNAME record, but you can create an alias record both for the root domain, such as example.com, and for subdomains, such as www.example.com. (You can create CNAME records only for subdomains.) When Route 53 receives a DNS query that matches the name and type of an alias record, Route 53 responds with the domain name that is associated with your distribution.

Option B is incorrect since you can't use S3 behind the Application Load balancer

Option D is incorrect because you need to define an ALIAS record

For more information on routing to Cloudfront, one can visit the below URL

- https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html (https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-to-cloudfront-distribution.html)

Ask our Experts

QUESTION 62 UNATTEMPTED

MANAGE, OPTIMIZE, AND TROUBLESHOOT THE NETWORK

A windows machine in one VPC needs to join the AD domain in another VPC. VPC Peering has been established. But the domain join is not working. What is the other step that needs to be followed to ensure that the AD domain join can work as intended

- **A.** Change the VPC peering connection to a VPNconnection
- **B.** Change the VPC peering connection to a Direct Connect connection
- **C.** Ensure the security groups for AD hosted instance has the right rules for relevant instances. ✔
- **D.** Ensure that the AD is placed in a public subnet

Explanation :

Answer – C
In addition to VPC peering and setting the right route tables , the security groups for the AD EC2 instance needs to ensure the right rules are put in place for allowing incoming traffic.
Option A and B is invalid because changing the connection type will not help. This is a problem with the Security Groups.
Option D is invalid since the AD should not be placed in a public subnet
For more information on allowing ingress traffic for AD, please visit the following url

- https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html (https://docs.aws.amazon.com/quickstart/latest/active-directory-ds/ingress.html)

Ask our Experts

QUESTION 63 UNATTEMPTED DESIGN AND IMPLEMENT AWS NETWORKS

Which of the following is a key prerequisite for creating an AWS Managed Microsoft AD directory? Choose 2 answers from the options given below

- [ ] **A.** AVPC with 2 subnets ✔
- [ ] **B.** Usage of a NAT Instance in the VPC
- [ ] **C.** Opening of several ports including port 53 ✔
- [ ] **D.** ANAT gateway in the public subnet

Explanation :

Answer – A and C
The AWS Documentation mentions the following
To create an AWS Managed Microsoft AD directory, you need a VPC with the following:

- At least two subnets. Each of the subnets must be in a different Availability Zone.
- The following ports must be open between the two subnets that you deploy your directory into. This is necessary to allow the domain controllers that AWS Directory Service creates for you to communicate with each other. A security group will be created and attached to your directory to enable communication between the domain controllers.
  - TCP/UDP 53 - DNS
  - TCP/UDP 88 - Kerberos authentication
  - UDP 123 - NTP
  - TCP 135 - RPC
  - UDP 137-138 - Netlogon
  - TCP 139 - Netlogon
  - TCP/UDP 389 - LDAP
  - TCP/UDP 445 - SMB
  - TCP 636 - LDAPS (LDAP over TLS/SSL)
  - TCP 873 - Rsync
  - TCP 3268 - Global Catalog
  - TCP/UDP 1024-65535 - Ephemeral ports for RPC
- The VPC must have default hardware tenancy.
- You cannot create a AWS Managed Microsoft AD in a VPC using addresses in the 198.19.0.0/16 address space.
- AWS Directory Service does not support using Network Address Translation (NAT)

with Active Directory. Using NAT can result in replication errors.

Options B and D are clearly invalid because it is clearly mentioned that NAT should not be used.
For more information on the pre-requisites, please visit the following url

- https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_prereqs.html (https://docs.aws.amazon.com/directoryservice/latest/admin-guide/ms_ad_getting_started_prereqs.html)

Ask our Experts

QUESTION 64 UNATTEMPTED

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company currently has a set of EC2 Instances hosted in a VPC. The IT Security department is suspecting a possible DDos attack on the instances. What can you do to zero in on the IP addresses which are receiving a flurry of requests.

- **A.** Use VPC Flow logs to get the IP addresses accessing the EC2 Instances ✔
- **B.** Use AWS Cloud trail to get the IP addresses accessing the EC2 Instances
- **C.** Use AWS Config to get the IP addresses accessing the EC2 Instances
- **D.** Use AWS Trusted Advisor to get the IP addresses accessing the EC2 Instances

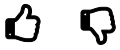
Explanation :

Answer – A

With VPC Flow logs you can get the list of IP addresses which are hitting the Instances in your VPC. You can then use the information in the logs to see which external IP addresses are sending a flurry of requests which could be the potential threat for a DDos attack.
Option B is invalid this is an API monitoring service and will not be able to get the IP addresses
Option C is invalid this is a config service and will not be able to get the IP addresses
Option D is invalid because this is a recommendation service and will not be able to get the IP addresses
For more information on VPC Flow Logs, please visit the following 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 65 INCORRECT

DESIGN AND IMPLEMENT FOR SECURITY AND COMPLIANCE

Your company has a set of EC2 Instances that are placed behind an ELB. Some of the applications hosted on these instances communicate via a legacy protocol. There is a security mandate that all traffic between the client and the EC2 Instances need to be secure. How would you accomplish this?

- **A.** Use an Application Load balancer and terminate the SSL connection at the ELB ✖
- **B.** Use a Classic Load balancer and terminate the SSL connection at the ELB
- **C.** Use an Application Load balancer and terminate the SSL connection at the EC2 Instances

○ **D.** Use a Classic Load balancer and terminate the SSL connection at the EC2 Instances ✔

Explanation :

Answer – D
Since there are applications which work on legacy protocols, you need to ensure that the ELB can be used at the network layer as well and hence you should choose the Classic ELB. Since the traffic needs to be secure till the EC2 Instances , the SSL termination should occur on the Ec2 Instances.
Option A and C are invalid because you need to use a Classic Load balancer since this is a legacy application.
Option B is incorrect since encryption is required until the EC2 Instance
For more information on HTTPS listeners for classic load balancers, please refer to below URL

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

Ask our Experts

Finish Review (https://www.whizlabs.com/learn/course/aws-cans-practice-tests/quiz/14784)

- 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/)

- Blog (https://www.whizlabs.com/blog/)

Mobile App

- Android Coming Soon
- iOS Coming Soon

Follow us

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

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

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

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