AWS CERTIFIED ADVANCED NETWORK SPECIALITY ANS-C01

Mock Examination

DILIP BAVISKAR
Baviskar.dilip@gmail.com

AWS ANS-C01 Examination Q & A

Domain: Network Design

1. A large telecom company has created Fifteen VPCs in different regions for deploying its IT servers. This VPC is created for each department like Accounts, Finance, Sales, Pre-Sales, and HR. A Central VPC is created which hosts servers accessed by all other VPCs. There is an additional requirement of servers in Accounts VPC communicating with servers in Finance VPC. IT Head wants you to ensure proper isolation between VPC & no additional reachability, including the internet, should be established. Which of the following solution will meet this requirement?

   A> Create a Mesh configuration on VPC Peering between Central VPC & all other VPCs. Create an additional VPC Peering between Accounts & Finance VPC for communication between them.

   B> Create a Full Mesh configuration on VPC Peering between all VPCs.

   C> Create a full mesh configuration on VPC peering between Central, Finance & Accounts VPC. Create a full VPC peering between Central VPC & all other VPCs.

   D> Create a VPN Connection between instances in Accounts & Finance VPC. Create a partial VPC peering between Central VPC & all other VPC.

   Explanation:

   Correct Answer - A

   Mesh configuration on VPC can be used to connect VPC with Central VPC so that all VPC can connect to servers in central VPC. With Mesh configuration (not a full mesh, but a partial mesh) on VPC, there would not be communication between all other VPCs. Since there are additional connectivity requirements between Finance & Account VPC, an additional peering can be established between these two VPCs.

   Options B&C are incorrect as creating a full mesh configuration between all VPCs will allow communication between all VPCs.

   Option D is incorrect as a VPN connection will be internet which is against the requirement.

   For more information on VPC Peering options, refer to the following URLS

   https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/amazon-vpc-to-amazon-vpc-connectivity-options.html

   https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/amazon-vpc-to-amazon-vpc-connectivity-options.html

Domain: Network Implementation

2. As an AWS consultant, you have been assigned to automate the VPC creation process. You successfully performed POC at the ap-northeast-1 region using AWS CloudFormation Template. With this template, you have created a VPC with public & private subnets with CIDR range along with an Internet Gateway. You need to replicate the same template in other regions for deployment. Which of the following can be used to incorporate the CIDR range of the region to the template so that users in each region can select these values?

A> Create Reference in AWS CloudFormation to allow users in different regions to specify region-specific CIDR ranges during Stack creation.

B> Use Parameters in AWS CloudFormation to allow users in different regions to specify region- specific CIDR ranges during Stack creation.

C> Use Functions Fn::Cidr in AWS CloudFormation to allow users in different regions to specify region-specific CIDR ranges during Stack creation.

D> Use Functions Fn::Select in AWS CloudFormation to allow users in different regions to specify region-specific CIDR ranges during Stack creation.

Explanation:

Correct Answer - B

Template Parameters can be used to customize Resource Properties in a template so that these templates can be re- used in deployment in other regions. In the above case, with Template Parameters, users can specify the CIDR range of a specific region while creating a stack.

Option A is incorrect as Reference will return physical ID for the resources. This will be used to refer to parameter values in a template.

Option C is incorrect as Fn::Cidr can be used to create smaller CIR blocks for a specified count & size from a larger CIDR block. This cannot be used to specify the CDR range during Stack creation.

Option D is incorrect as Fn::Select can be used to select one value from a range of values in a function.

Domain: Network Security, Compliance, and Governance

3. A manufacturing firm is storing all project documents in various S3 buckets. Application servers deployed within a VPC need to access these S3 buckets to fetch the latest files. To limit servers with Internet access, the client has created Amazon S3 endpoint to have secure access to the S3 bucket. The client needs to further

enhance security by having control over individual Servers accessing only authorized S3 buckets (using role-based access on a bucket policy) and should be denied from accessing all other S3 buckets. Which of the following can be used to meet this requirement?

A> Create a VPC endpoint policy that restricts access to specific S3 buckets only.

B> Create an S3 bucket policy with aws:Sourcelp condition matching instance IP address to control access from each server to S3 bucket.

C> Create an outbound security group rule which specifies a prefix list for the S3 bucket from each server.

D> Create an outbound NACL that specifies a prefix list for the S3 bucket from each server.

Explanation:

Correct Answer - A

A VPC endpoint policy is an IAM resource policy that you attach to an endpoint when creating or modifying the endpoint. If you do not attach a policy when you create an endpoint, we attach a default policy for you that allows full access to the service. If a service does not support endpoint policies, the endpoint allows full access to the service. An endpoint policy does not override or replace IAM user policies or service-specific policies (such as S3 bucket policies). It is a separate policy for controlling access from the endpoint to the specified service.

Domain: Network Security, Compliance, and Governance

4. A secure payment application is deployed on the EC2 instance in VPC. This application server is accessed by the internal team & vendors for uploading security patches. You have a security group policy that allows only SSH to this application from all IP subnets. The Security Team needs to get notified when more than Fifty SSH login attempts were recorded from unknown IP addresses in an hour. Which of the following solution can be deployed with the least cost to meet this requirement?

A> Create a VPC Flow logs for the Server network interface. Export flow logs to Amazon S3 bucket with Lifecycle management policies. Create a CloudWatch alarm for this bucket which will notify the Security Team when a number of failed SSH login attempts breaches the threshold value.

B> Create a VPC Flow logs for VPC in which the Server instance is launched. Export flow logs to Amazon S3 bucket with Lifecycle management policies. Create a CloudWatch alarm for this bucket which will notify the Security Team when a number of failed SSH login attempts breaches the threshold value.

C> Create a VPC Flow logs for VPC in which the Server instance is launched. Export flow logs to CloudWatch Logs. Create a cloudwatch metric and trigger an alarm that will notify the Security Team when a number of failed SSH login attempts breaches the threshold value.

D> Create a VPC Flow logs for the Server network interface. Export flow logs to CloudWatch Logs. Create a Cloudwatch metric and trigger an alarm that will notify the Security Team when a number of failed SSH login attempts breaches the threshold value.

Explanation:

Correct Answer - D

Flow Logs can be published to CloudWatch logs to set alarms for specific notifications. There are charges involved when flow log data is saved in either S3 buckets or published to CloudWatch. So, in order to have a cost-effective solution, you can enable Flow logs only on a specific instance interface & published them to CloudWatch.

Options A & B are incorrect as this is not an effective way to store data in the S3 bucket & again publish it to CloudWatch. Instead of that, direct flow logs can be published to CloudWatch & an alarm can be set to notify Security Team.

Option C is incorrect as although this will work in capturing failed SSH login attempts to the Server network interface, these flow logs will capture logs for all interface & subnets within that VPC. When a large amount of data is published to CloudWatch logs, this will incur additional charges.

For more information on using Flow Logs, refer to the following URL

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-cwl.html#flow-logs-cwl-create-flow-log

Domain: Network Implementation

5.A global airline company uses hybrid connectivity for application servers deployed in high availability mode in both on-premises & VPC. They have created VPC A & VPC B spread across three Availability Zones for deploying multiple servers. The airline IT team is planning to set up a new DNS server at on-premises locations. Servers in both VPC A & VPC B will need to forward queries to new DNS servers. IT Head is looking to implement the least complex solution which can be implemented with case. As AWS consultants, they are looking for your guidance to implement this solution with the least management overhead & low cost.

Which of the following solutions can be deployed to meet this requirement?

A>Configure Route 53 Resolver with an outbound endpoint in VPC A & forwarding rules shared with VPC B

B> Configure Route 53 Resolver with an inbound endpoint in VPC A & forwarding rules shared with VPC B.

C> Configure Distributed forwarders on each instance within VPN A & VPC B which would forward queries to on-premises DNS servers.
D> Configure Zonal forwarders on multiple instances within VPN A & VPC B which would forward queries to on-premises DNS servers.

Explanation:

Correct Answer - A

Route 53 Resolver can be set up easily with low cost to forward DNS queries between on-premises & VPC. In the above case, since DNS servers at on-premises locations need to be used for servers deployed in VPC, a Route 53 Resolver outbound endpoint needs to be set up with forwarding rules. This outbound endpoint is not required to be created for each VPC, but a single endpoint can be shared between multiple VPCs. There is no management overhead with this outbound endpoint, as once it's set up, you just need to manage forwarding rules.

Option B is incorrect as Inbound endpoints can be used to forward queries from on-premises into VPC.

Option C is incorrect as configuring DNS forwarders on all instances will require additional admin work.

Option D is incorrect as implementing Zonal Forwarders is complex & will incur a higher cost than Router 53 Resolver Outbound endpoint.

For more information on using AWS Route 53 Resolver, refer to the following URL •

https://dl.awsstatic.com/whitepapers/hybrid-cloud-dns-options-for-vpc.pdf

https://dl.awsstatic.com/whitepapers/aws-hybrid-dns-with-active-directory.pdf

Domain: Network Implementation

6. An online educational institute is using Hybrid architecture for its application servers. They use existing DNS servers deployed at on-premises data centers to resolve queries from servers hosted in VPC. Outbound Endpoints are created for this purpose for the entire domain name resolution. A new subdomain is created for testing new training programs. Dcv-ops teams do not want on-premise DNS servers to resolve queries for this subdomain, but it should be handled locally within VPC.

Which of the following rules can be configured to use a separate DNS server for a new subdomain?

A> Create a custom rule for the new subdomain.
B> Create a conditional forwarding rule for the new subdomain.
C> Create a system rule for the new subdomain.
D> Create a recursive rule for the new subdomain.

Explanation:

Correct Answer - C

By creating System rules, specific subdomains are resolved locally by resolvers instead of forwarding these queries to on-premises DNS servers. When conditional forwarding rules are created for a domain, it would apply to domains & all subdomains forward to on-premises DNS resolvers. System rules can be created to override this behavior for one of the sub-domain & resolve it locally.

Option A is incorrect as Custom rules are of a single type which is conditional forwarding rules. These would forward all requests to an on-premises DNS resolver.

Option B is incorrect as Conditional Forwarding rules would forward all requests to on-premises DNS resolver.

Option D is incorrect as Resolver automatically creates recursive rules for all domains not created by custom rules.

For more information on creating rules for AWS Route 53 Resolver, refer to the following URL

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html

Domain: Network Implementation

7. A food production company is having hybrid connectivity between regional Data Centro & AWS VGW using AWS Direct Connect link. VPC A & VPC B is created to deploy multiple servers accessed by users in regional offices. A private hosted zone is created for a new domain hosted on one of the servers in VPC B. Route 53 Resolver inbound endpoint is created in VPC A for a large volume of DNS queries from users in regional offices. These users are complaining of DNS queries failing for domains created in a private hosted zone but working for other domains hosted in VPC.

Which of the following actions need to be taken to resolve the issue?

A> The existing Inbound endpoint is loaded, implementing another inbound endpoint in VPC A to cater traffic from on-premises users to private hosted zones.
B> VPC pooring needs to be enabled between VPC A & VPC B
C> Private Hosted Zone needs to be created in VPC A, where an inbound endpoint is created.
D> cnableDnsHostnames & enableDnsSupport need to be enabled in VPC A.

Explanation:

Correct Answer - C

It should be in the same VPC where Route 53 Resolver inbound endpoint is created for Private Hosted zones. In the above case, Route 53 Resolver inbound endpoint is created in VPC A. So, a private hosted zone needs to be created in this VPC A.

• Option A is incorrect as Creating another endpoint in VPC A will not resolve issues faced by users for private hosted zones in VPC B. Also, for loaded endpoints, the best practice is to add an additional IP address to the endpoint instead of creating a new endpoint.

• Option B is incorrect as VPC peering is not required to be enabled for sharing inbound endpoints between VPCs.

• Option D is incorrect as these attributes need to be set for the VPC to enable DNS resolution on instances launched within VPC. These attributes will be required at VPC, but this will not cause query failures for on- premises users to sub-domain names.

For more information on AWS Route 53 Resolver inbound endpoints, refer to the following URL

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html#resolver-considerations-inbound-endpoint-private-zone

Domain: Network Design

8. Each division within a start-up organization has a separate account & has created a separate VPC for deploying its servers. They have a regional office having existing internet links over which they are planning to access these servers for management purposes. All servers between those VPC need to have connectivity established between them. The CTO of this fastest growing startup is looking for a fully managed high available & scalable solution considering future growth in the number of VPCs.

Which of the following design approaches can be implemented to meet this requirement?

A. Create VPC Peering between all these VPCs & Create a single VPN connection from the regional office to one of the VPC.

B. Create VPC Peering between all these VPCs & Create multiple VPN connections from regional offices to cach of the VPC to which it needs to communicate.

C. Create a Transit Gateway with all VPC attached to it & create a single VPN connection from the regional office to one of the VPC.

D. Create a Transit Gateway with all VPC attached to it & create a single VPN connection from the regional office to Transit Gateway.

Explanation:

Correct Answer - D

Transit gateway can be deployed to have full-mesh connectivity between multiple VPC & on-premises connectivity either via VPC connection or AWS Direct Connect connections. It is a fully managed service providing high availability & scalability for an increase in the number of VPC in the future.

• Option A is incorrect as VPC peering can be done for a small number of VPC. There would be additional overhead for a large number of VPC to implement manage multiple peering connections.

• Option B is incorrect as Creating a VPN connection with all VPC is not a viable solution. The VPN connection can be created with transit Gateway through which it can communicate with all VPCs.

• Option C is incorrect as VPN connections need to be created with the Transit gateway & not to a VPC.

For more information on AWS Transit Gateway, refer to the following URL

https://aws.amazon.com/transit-gateway/features/

Domain: Network Design

9. An IT firm has created multiple VPCs as per project requirements which have customers' application servers deployed. The firm is planning to deploy a Direct Connect Link from its multiple offshore locations which need to access servers from VPC for monitoring & troubleshooting purposes. IT firm is looking for a highly available solution that can control traffic between VPC so that only specific subnets within those VPC can communicate with each other. As an AWS consultant, you have suggested implementing Transit Gateway & AWS Direct Connect Gateway.

Which of the below additional considerations should be followed while implementing the above suggestion sufficing client requirement?

A> Create separate subnets for each Transit gateway VPC attachments & enable BGP route propagations for AWS Direct Connect gateway attachments.

B> Create separate subnets for each Transit gateway VPC attachments & create an additional Transit Gateway for high availability.

C> Create a single subnet for each Transit gateway VPC attachments & enable BGP route propagations for AWS Direct Connect gateway attachments.

D> Create a single subnet for each Transit gateway VPC attachments & create an additional Transit Gateway for high availability.

Explanation:

Correct Answer - A

AWS Transit Gateway can be deployed to create full mesh or isolate VPC communication between VPC connecting to it

as well as on-premises connectivity over AWS Direct Connect or VPN connections. Also, route propagation should be

enabled for BGP routes from offshore locations to communicate with servers in all VPC.

• Option B is incorrect as an additional Transit gateway is not required as Transit gateway is by design highly available.

• Options C & D are incorrect as configuring a single subnet for Transit gateway VPC attachments is not recommended.

For more information on AWS Transit Gateway, refer to the following URL

https://docs.aws.amazon.com/vpc/latest/tgw/tgw-best-design-practices.html

Domain: Network Design

10. A large electrical appliance firm is using AWS Cloud infrastructure for deploying application servers. It has created 3 VPC R&D, VPC Production & VPC IT. VPC IT has shared services servers deployed which need to have communication with servers in all three VPC. As per corporate guidelines, VPC R&D VPC Production should be able to communicate with VPC IT, but there should not be any communication between VPC R&D & VPC Production. To support future demand in the number of VPC, the Transit gateway is deployed to have communication between these VPC.

Which of the following route table configuration on Transit Gateway will you design to meet this requirement?

A> Create Two Routing tables in Transit Gateway. Associate VPC R&D & VPC IT attachments to one route table having routes propagated from cach VPC. Associate VPC Production & VPC IT attachments to one route table having routes propagated from each VPC.

B> Create Two Routing tables in Transit Gateway. Associate VPC R&D, VPC Production attachments to the route table having routes propagated from VPC IT. Associate VPC IT attachments with route tables having propagated routes from VPC R&D & VPC Production.

C> Create Two Routing tables in Transit Gateway. Associate VPC R&D, VPC Production attachments to the route table having static default route. Associate VPC IT attachments with route tables having propagated routes from VPC R&D & VPC Production.

D> Create Two Routing tables in Transit Gateway. Associate VPC R&D, VPC Production attachments to default route table having route propagation enabled. Associate VPC IT attachments with route tables having propagated routes from VPC R&D & VPC Production.

Explanation:

Correct Answer - B

Transit Gateway can be used for isolated shared services between multiple VPCs. For this, two routing tables can be created in Transit Gateway. First, the route table would have a route table with routes propagated from VPC R&D & VPC Production attachments. Other route tables would have a route table with routes propagated from VPC IT.

Option A is incorrect as For Transit Gateway, cach attachment can be associated only to one route table. In the above casc, VPC IT cannot be associated with two route tables. Option C is incorrect as with the static Default route. Both VPC R&D & PC Finance will be able to communicate with cach other. Option D is incorrect as with the default route table, VPC R&D & VPC Production will be able to communicate with cach other.

For more information on AWS Transit Gateway, refer to the following URL

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated-shared.html

11. A global pharma firm has deployed multiple application servers on AWS EC2 instances in the us-west-1 region. Corporate Office based in California has a Direct Connect Link to VGW in the us-west-1 region to access these application servers. The firm is expanding its presence in the Asia regions with new offices in Mumbai & Tokyo. The team plans to deploy new application servers on Amazon EC2 instances launched in ap-south-1 & ap-northeast-1 regions for this developer. All these servers will be working independently & will be catering to users in specific regions where it's hosted. Corporate users will be accessing servers in all three VPC from the corporate office. The firm is looking for a cost-effective scalable solution that is easy to manage to provide this connectivity.

Which of the following can be created to meet this requirement?

A> Create a new Public VIF on AWS Direct Connect link in the us-west-1 region. Create a VPN Connection over this Public VIF to a VGW attached to ap-south-1 & ap-northeast-1 to access application servers.

B> Create a new private VIF on the AWS Direct Connect link in the us-west-1 region. Connect to VGW created in ap-south-1 & ap-northeast-1 regions using this private VIF to access application servers.

C> Create a new private VIF on the AWS Direct Connect link in the us-west-1 region. Associate this private VIF with Direct Connect Gateway to connect to VGW attached to ap-south-1 & ap-northeast-1 regions.

D> Create a new public VIF on the AWS Direct Connect link in the us-west-1 region. Associate this public VIF with Direct Connect Gateway to connect to VGW attached to ap-south-1& ap-northeast-1 regions.

Explanation:

Correct Answer – C

A Direct Connect Gateway can be used to connect to VGW globally. A private VIF is created over AWS Direct Connect connection in this setup, which will have a single BGP peering with AWS Direct Connect gateway. Further, this AWS Direct Connect gateway is associated with VGW attached to VPC created in different regions. In the above case, the customer can use the existing AWS Direct Connect link to connect to the AWS Direct Connect gateway & then create associations with VGW ap-south-1 & ap-northeast-1 regions.

• Option A is incorrect as Although this will work, creating VPC for connecting to each VPC will incur additional cost & admin work.

• Option B is incorrect as Private VIF can be connected to VGW in the local region where AWS Direct Connect is connected & cannot be used to connect to VGW in other regions.

• Option D is incorrect as For the AWS Direct Connect link, private VIF & not public VIF needs to be created to connect to the AWS Direct Connect gateway which in turn associate with multiple VGW attached to VPC.

For more information on the Direct Connect gateway, refer to the following URL https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

12. A finance institute has deployed its application servers in multiple VPCs created in us-east-1 & us-west-1 regions. Developer Team based at head office are accessing these servers over 10 Gig AWS Direct Connect connections in the us-east-1 region which is attached to the Direct Connect gateway associated with VGW in each VPC. They are planning to launch a new banking application for which they have deployed new servers in additional VPC's created in us-east-1 & us-west-1 regions. The developer team requires high performance connectivity with new servers from the on- premises location in addition to connectivity to existing servers. Also, servers in all VPC need to have connectivity with each other for data synchronization.

Which of the following designs needs to be implemented to meet this requirement?

A> Remove the existing association between AWS Direct Connect Gateway & VGW. Connect all VPCs to the Transit Gateway. Create a new association between Transit Gateway & Direct Connect gateway over the private virtual interface.

B> Retain existing association between AWS Direct Connect Gateway & VGW. Connect new VPCs to Transit Gateway. Create a new association

between Transit Gateway & Direct Connect gateway over the private virtual interface.

C> Retain existing association between AWS Direct Connect Gateway & VGW. Connect all VPCs to the Transit Gateway. Create a new association between Transit Gateway & Direct Connect gateway over transit virtual interface.

D> Remove the existing association between AWS Direct Connect Gateway & VGW. Connect all VPCs to the Transit Gateway. Create a new association between Transit Gateway & Direct Connect gateway over transit virtual interface.

Explanation:

Correct Answer - D

AWS Direct Connect Gateway cannot be associated with Transit Gateway when it's associated with VGW. In the above requirements, servers in all VPC need to have connectivity with each other. This can be established by connecting all VPC to Transit Gateway. To enable connectivity from head office to servers in all VPC, a transit virtual interface needs to be created to connect AWS Direct Connect gateway with Transit gateway.

• Options A & B are incorrect as AWS Direct Connect Gateway needs to connect to Transit gateway over transit virtual interface & not private virtual interface.

• Option C is incorrect as AWS Direct Connect gateway cannot be associated with Transit Gateway while it's already connected to VGW.

For more information on the Direct Connect gateway, refer to the following URL

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

Domain: Network Design

13. A media firm has created Sales VPC, Marketing VPC & Media VPC. Media VPC has many servers hosting large size media content uploaded from an on-premises office. Users from on-premises offices also need to have access to Sales VPC & Marketing VPC. Servers in Marketing VPC download media content from Media VPC on a regular basis to create modified content for external clients. Sales VPC should be isolated from Media VPC & Marketing VPC with only need basis specific subnets to access these VPCs. The firm is looking for a cost-effective, scalable solution to be deployed.

As an AWS Architect, which of the following will you suggest implementing to meet the requirement?

A> Create Private VIF over AWS Direct Connect Gateway to Media VPC. Create full mesh VPC peering between Sales, Marketing & Media VPC. Create a VPN connection from on-premises to each of the VPC for communication between on-premises users & each of the three VPC.

B> Create Transit VIF over AWS Direct Connect Gateway to connect to Transit Gateway which will have an association with specific subnets from all three VPC. Create a VPC peering between Marketing VPC & Media VPC.

C> Create Private VIF over AWS Direct Connect Gateway to Media VPC. Create Transit VIF over another AWS Direct Connect Gateway to connect to Transit Gateway which will have an association with specific subnets from all three VPC. Create a VPC peering between Marketing VPC & Media VPC.

D> Create Transit VIF over AWS Direct Connect Gateway to connect to Transit Gateway which will have an association with specific subnets from all three VPC. Create a full mesh VPC peering between Sales, Marketing & Media VPC.

Explanation:

Correct Answer - C

From On-premise to Media VPC, large size videos files need to be uploaded so Private VIF over AWS Direct Connect Gateway would provide dedicated bandwidth & minimize cost as compared to having connectivity via Transit gateway. To limit traffic flowing via Transit Gateway for servers between Marketing VPC & Media VPC, VPC peering can be implemented without hourly connection charges as in Transit Gateway. For specific IP communication between Sales, Marketing & Media VPC & with on-premise users, a transit Gateway can be deployed.

• Option A is incorrect as creating VPC peering between all three VPC will allow Sales VPC full access to the other two VPC. Also, creating a separate VPN from on-premises to each of three VPC will be a costly & non-scalable solution.

• Option B is incorrect as using Transit Gateway for heavy traffic between on-premises to Media VPC will incur a huge cost compared to having Private VIF connectivity from AWS Direct Connect gateway to Media VPC.

• Option D is incorrect as using Transit Gateway for heavy traffic between on-premises to Media VPC will incur a huge cost compared to having Private VIF connectivity from AWS Direct Connect gateway to Media VPC. Also, with full mesh VPC peering, it would be a non-scalable solution.

For more information on Hybrid Connectivity, refer to the following URL

https://dl.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf

Domain: Network Design

14. A multinational banking institute is using AWS infrastructure for deploying its application servers. A new application is being developed on a fleet of EC2 servers in VPC spread across multiple AZ & will be having ALB in the front-end. Global users would be accessing this banking application which needs to be highly secure & high-performance. The security team is concerned about the security of this application & needs a new solution to mitigate DDoS attacks.

Which of the following solutions will meet the requirement?

A> Create an internal ALB in a VPC with an internet gateway attached & without any Public IP address assigned to it. Associate ALB as an endpoint in AWS Global Accelerator.

B> Create an internal ALB in a VPC with an internet gateway attached & with Public IP address assigned to it. Associate ALB as an endpoint in AWS Global Accelerator.

C> Create an internal ALB in a VPC without an internet gateway attached & with an Elastic IP address assigned to ALB. Associate ALB as an endpoint in AWS Global Accelerator.

D> Create an internal ALB in a VPC without an internet gateway attached & a Private IP address assigned to ALB. Associate ALB as an endpoint in AWS Global Accelerator.

Explanation:

Correct Answer - A

When ALB is used as an endpoint for AWS Global Accelerator, all traffic towards this endpoint flows over AWS Global Accelerator. For this, a public IP address is not required to be assigned to ALB, but an internet gateway is required to be attached to VPC to indicate internet traffic is accepted in this VPC. With Internet traffic flowing only via a single-entry point of AWS Global Accelerator, it will help reduce DDoS attacks.

• Option B is incorrect as with internal ALB used as an endpoint for AWS Global Accelerator, Public IP not required to be assigned to ALB.

• Options C & D are incorrect as Internet Gateway needs to be attached to VPC with an internal ALB created.

For more information on Secure VPC connections in AWS Global Accelerator, refer to the following URL

https://docs.aws.amazon.com/global-accelerator/latest/dg/secure-vpc-connections.html

Domain: Network Design

15. An IT company is using AWS Infrastructure in the us-west-1 region for deploying application servers across multiple VPC. Recently this company has expanded its

geographical presence & acquired two startup firms in the Singapore & Sydney region. Since there is no dedicated bandwidth requirement, a secure VPN connection is established from these offices to VPC in the us-west-1 region to allow users in remote offices to access applications. Users are complaining of slow access to applications which is impacting their work &, in turn, affecting business. The CTO of this company is looking for performance improvement which should enhance remote user experience while accessing those applications.

Which of the following solutions can be deployed quickly if cost is not a constraint?

A> Create an AWS Direct Connect connection in each Singapore & Sydney region. Create a VPN connection over this link to VPC in the us-west-1 region.

B> Create an attachment from each VPC in the us-west-1 region to AWS Transit Gateway. Delete existing VPN connection from Singapore & Sydney office & create a new VPN Connection with attachments to transit gateway with acceleration enabled.

C> Create AWS Direct Connect connection in each Singapore & Sydney region with Private VIF associating with AWS Direct Connect gateway. Associate this AWS Direct Connect gateway with VPC in the us-west-1 region.

D> Create a new VGW in each VPC in the us-west-1 region. Delete existing VPN connection from Singapore & Sydney office & create a new VPN Connection to VGW in each VPC at us-west-1 with acceleration enabled.

Explanation:

Correct Answer - B

VPN connections with acceleration enabled use AWS Global Accelerator to improve performance of VPN tunnels. With acceleration enabled, VPN tunnels are formed with static IP address of nearest edge location & from edge location ormad traffic is moved over AWS global backbone infrastructure to reach VPC in the destination region. A transit gateway is required to be created as Accelerated VPN connections only support termination on transit gateway & not on Virtual private gateway.

• Options A & C are incorrect as there is no dedicated bandwidth requirement. Using AWS Direct Connect links is not the best option.

• Option D is incorrect as VPN Connection with acceleration is not supported with virtual private gateway & is supported only as an attachment with transit gateway.

For more information on Accelerated VPN connection with AWS Global Accelerator, refer to the following URL

https://aws.amazon.com/blogs/architecture/improve-vpn-network-performance-of-aws-hybrid-cloud-with-global-accelerator/

Domain: Network Design

16. A tractor manufacturing firm is using SCADA control systems architecture for its manufacturing plants. These systems require low latency to application servers deployed in AWS infrastructure. To meet this requirement, they plan to deploy AWS Outposts deploying application servers within their IT facility at manufacturing plants. The firm is seeking your guidance for provisioning AWS Outposts parenting to the nearest AWS region for management traffic & there should be no impact on connectivity from manufacturing plants to other servers deployed in VPC.

Which of the following suggestions will you provide to build this connectivity? (Select Two.)

A>Create a Service Link Path.
B> Create Local Gateway Path.
C> Create a Private VIF over AWS Direct Connect to communicate with AWS IP ranges.
D> Use internet Link to communicate with AWS IP ranges.
E> Advertisement of AWS Outposts Subnet to Local gateway.

Explanation:

Correct Answer - A, D

While AWS Outposts is provisioned, it requires connectivity to public AWS ranges in the nearest AWS region either over the internet or AWS Direct Connect Public VIF. Service Link path can be deployed for this serving two things- Management traffic to the AWS Outpost & traffic from AWS Outposts to other services in AWS cloud.

• Option B is incorrect as Local Gateway Path is for traffic between AWS Outpost & On-premises network & not for management traffic towards parent region.

• Option C is incorrect as For Management traffic, AWS Outposts should be able to connect with AWS public subnets. For this, a Public VIF needs to be created with AWS Direct Connect & Not private VIF.

• Option E is incorrect as this advertisement is required for connectivity from AWS Outpost to on-premises subnets.

For more information on AWS Outposts, refer to the following URLS

https://docs.aws.amazon.com/outposts/latest/userguide/region-connectivity.html

https://pages.awscloud.com/AWS-Outposts-Networking-Foundations_2020_0010-CMP_OD.html

17. A media company uses hybrid connectivity to access video editing applications deployed on EC2 instances launched in custom VPC in the us-west-1 region. Employees access these applications for uploading live production videos. Recently there are complaints of high latency while accessing these applications from employees. The company has decided to set up AWS Local Zones to mitigate the latency issue. Project Team deploying AWS Local zones is concerned about the IP address to be used for new EC2 instances in AWS Local Zones.

Which of the following can be recommended for IP address assignment for EC2 instances in AWS Local Zones?

A> Enable Local Zone in us-west-1 region Extend existing subnet from VPC created in parent region to AWS Local Zones. Assign an IP address for an EC2 instance in AWS Local Zones from this subnet.

B> Enable Local Zone in us-west-1 region. Create a new subnet from an existing VPC in the parent region. Assign this subnet to AWS Local Zones. Assign an IP address for an EC2 instance in AWS Local Zones from this subnet.

C> Enable Local Zone globally. Create a new subnet from an existing VPC in the parent region. Assign an IP address for an EC2 instance in AWS Local Zones from this subnet.

D> Enable Local Zone globally. Create a new subnet from an existing VPC in the parent region. Assign this subnet to AWS Local Zones. Assign an IP address for an EC2 instance in AWS Local Zones from this subnet.

Explanation:

Correct Answer - B

For creating AWS Local Zone, it needs to be enabled in a region & not globally. While creating a subnet in AWS Local Zones, subnets from parent VPC are extended to these AWS Local Zones.

• Option A is incorrect as a new subnet needs to be created from existing VPC & not existing subnet can be extended to AWS Local Zones.

• Option C is incorrect as the new subnet in the existing VPC needs to be allocated to AWS Local Zones before being used.

• Option D is incorrect as Local Zones need to be enabled in the us-west-1 region & not globally.

For more information on AWS Local Zones, refer to the following URL

https://aws.amazon.com/blogs/compute/low-latency-computing-with-aws-local-zones-part-1/

18. A global telecom firm is planning to launch a new application for its premium customers. This application requires ultra-low latency to EC2 application servers

hosted in AWS cloud infrastructure. All application data need to be uploaded to Database servers with optimum latency. IT Head is concerned for the end-to-end connectivity from mobile users to the application servers. As an AWS Consultant, you have been instructed to work on a solution to reduce the number of hops & ensure the latency threshold is committed to end-users. Which of the following can be deployed to meet the requirement?

A> Create an AWS Wavelength zone within the telecom provider facility & launch Amazon EC2 instance within this zone. Deploy Database servers in the parent region connecting to this AWS Wavelength.

B> Create an AWS Wavelength zone at the nearest edge location & launch Amazon EC2 instance within this zone. Deploy Database servers in the parent region connecting to this AWS Wavelength.

C> Create an AWS Wavelength zone at the nearest edge location & launch Amazon EC2 instance within this zone. Deploy Database servers in the same VPC created in the AWS Wavelength zone.

D> Create an AWS Wavelength zone within the telecom provider facility & launch Amazon EC2 instance within this zone. Deploy Database servers in the same VPC created in the AWS Wavelength zone.

Explanation:

Correct Answer - A

AWS Wavelength can be deployed with Telecom Provider IT infrastructure to provide low latency for mobile users to applications servers deployed on an EC2 instance within AWS cloud. With AWS Wavelength, Compute & Storage services can be launched. AWS Wavelength is connected back to the AWS region for communication with other AWS services. In the above case, application servers can be launched within the EC2 instance in AWS Wavelength deployed at telecom provider facility & database servers can be launched in AWS Region. **Option B is incorrect** as creating an AWS Wavelength at the edge location is not a valid option. **Option C is incorrect** as creating an AWS Wavelength at the edge location is not a valid option. Also, Database servers need to be deployed in the parent region & not in the AWS Wavelength zone. **Option D is incorrect** as Database servers should be created in the parent region & not in AWS Wavelength Zone.

For more information on AWS Wavelength, refer to the following URLs

https://aws.amazon.com/wavelength/faqs/

https://aws.amazon.com/wavelength/resources/

Domain: Network Management and Operation

19.A company has created VPC peering between VPC A in the us-east-1 region and VPC B in the us-west-1 region. A large number of Amazon EC2 instances are launched in both VPCs. For inter-VPC communication, a secondary private IPv4 address assigned to the network interface is used. Operations Head is looking for top-talker instances generating traffic within these VPCs. What actions can be initiated to get these details in the simplest way?

A>Create a flow log with the pkt-dstaddr field. Create a bucket in Amazon S3. Publish flow logs to this bucket. Use Amazon Athena to point logs in Amazon S3 and query the logs to get a list of top-talker instances.

B> Create a flow log with the dstaddr field. Create a bucket in Amazon S3. Publish flow logs to this bucket. Use Amazon Athena to point logs in Amazon S3 and query the logs to get a list of top-talker instances.

C> Create a flow log with the pkt-dstaddr field. Store flow logs to CloudWatch Logs. Use Amazon Athena to point logs in Amazon CloudWatch logs and query the logs to get a list of top- talker instances.

D> Create a flow log with the dstaddr field. Store flow logs to CloudWatch Logs. Use Amazon Athena to point logs in Amazon CloudWatch logs and query the logs to get a list of top- talker instances.

Explanation:

Correct Answer: A

In VPC flow logs, srcaddr and dstaddr fields in the log always display the primary private IPv4 address of the network interface. Suppose the Amazon EC2 instance uses a network interface with multiple IPv4 addresses. In that case, a pkt- dstaddr field in a VPC flow log can be used to display the destination IP address assigned as the secondary IP address. Amazon Athena can be used to query VPC flow logs stored in an Amazon S3 bucket. Amazon Athena has pre-defined queries like "VpcFlowLogsTopTalkingInstances" which provides ID's of the top 50 instances generating the most traffic. **Option B is incorrect** as the dstaddr field displays the primary IPv4 address of the network interface. It will not capture a packet destination if the packet has a destination other than the primary interface. **Option C is incorrect**. To query VPC flow logs using Amazon Athena, logs should be stored in the Amazon S3 bucket and not in CloudWatch logs. **Option D is incorrect** as the dstaddr field displays the primary IPv4 address of the network interface. It will not capture the packet destination. To query VPC flow logs using Amazon Athena, logs should be stored in the Amazon S3 bucket and not in CloudWatch logs.

For more information on querying flow logs for secondary interfaces using Amazon Athena, refer to the following URLs,

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs.html

https://docs.aws.amazon.com/vpc/latest/userguide/flow-logs-athena.html

Domain: Network Security, Compliance, and Governance

20. A global IT company has deployed its applications in the AWS cloud. Remote workers of this company are accessing Amazon workspaces deployed in a private subnet of the VPC. Internet access to Amazon Workspaces is provided via NAT Gateway attached to this VPC. The security head has instructed you to ensure security hardening is properly done. The solution deployed should be scalable and highly available and there should not be any impact on users accessing remotely.

What can be configured to meet security requirements?

A. Configure Amazon GuardDuty.

B. Configure Network Firewall.

C. Configure Security groups to Amazon Workspaces.

D. Configure Network ACL to the private subnet of the VPC.

Explanation:

Correct Answer: B

AWS Network Firewall is a stateful network firewall and intrusion detection and prevention service for the VPC. It works from layer 3 to layer 7 of the OSI layer. It can be used to filter traffic at the perimeter of the VPC for traffic coming from an Internet Gateway, NAT gateway, or from AWS VPN/Direct connect from an on-premises network. AWS Network Firewall is a managed solution that provides scalable and highly available solutions.

Option A is incorrect. Amazon Guard Duty is a threat detection service that continuously monitors and protects AWS accounts and data stored in the Amazon S3 bucket. This is not an ideal security solution for services launched within the VPC.

Option C is incorrect. The security group will work only for Layer 3 and layer 4; it won't be useful for securing layer 5 to layer 7 of the OSI layer.

Option D is incorrect. Network ACL works on a subnet level protecting all hosts in that subnet and working in layers 3-4. It won't be useful for securing layer 5 to layer 7 of the OSI layer.

For more information on AWS Network Firewall, refer to the following URLS,

https://docs.aws.amazon.com/network-firewall/latest/developerguide/what-is-aws-network-firewall.html

https://aws.amazon.com/blogs/security/protect-your-remote-workforce-by-using-a-managed-dns-firewall-and-network-firewall/

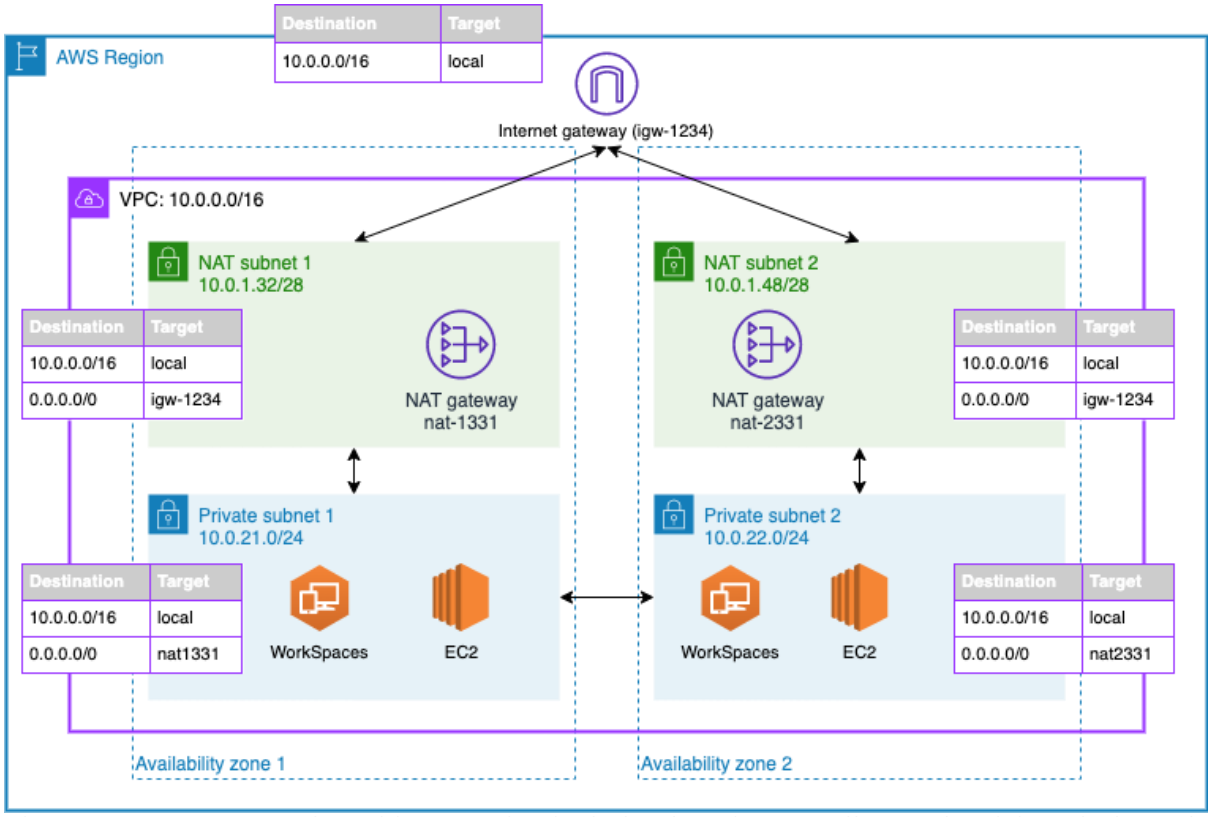


Figure 1: Q20 An example architecture that includes domain controllers and QuickBooks hosted on EC2 and Amazon WorkSpaces for user virtual desktops

21. A global pharma company uses Software-defined Wide Area Network (SD-WAN) to connect its global data center with all branch offices globally over the public internet. Recently they have deployed applications in AWS cloud at the eu- west-2 region. The company is looking for high bandwidth options to connect data centers and branch offices to the AWS cloud. This connectivity should utilize existing SD-WAN infrastructure. The proposed solution should have the least operational cost and be scalable to connect to any other AWS regions in which applications will be deployed in the future.

How can connectivity be designed to meet the purpose?

A> Set up IPsec VPNs between SD-WAN network virtual appliances and Transit Gateway. Configure BGP route propagation on the Transit gateway for routing traffic from an on- premises location to AWS.
B> Set up GRE VPN between SD-WAN network virtual appliances and Transit Gateway. Configure static routing on the Transit gateway for routing traffic from an on-premises location to AWS.
C> Set up AWS Transit Gateway with Connect attachment to SD-WAN virtual appliance. Configure BGP peering between these devices over the GRE tunnel.
D> Set up AWS Transit Gateway with Connect attachment to SD-WAN virtual appliance. Configure BGP peering between these devices over the IPsec tunnel.

Explanation:

Correct Answer: C

AWS Transit Gateway Connect is a new attachment type that can be used to connect SD-WAN to the AWS cloud. This supports GRE (Generic routing encapsulation) providing higher bandwidth performance. BGP peering can be created over the GRE tunnel to exchange routes between data center/branch offices with AWS. AWS Transit Gateway peering can be used for future connectivity with other regions. Connectivity will be as per the below diagram,

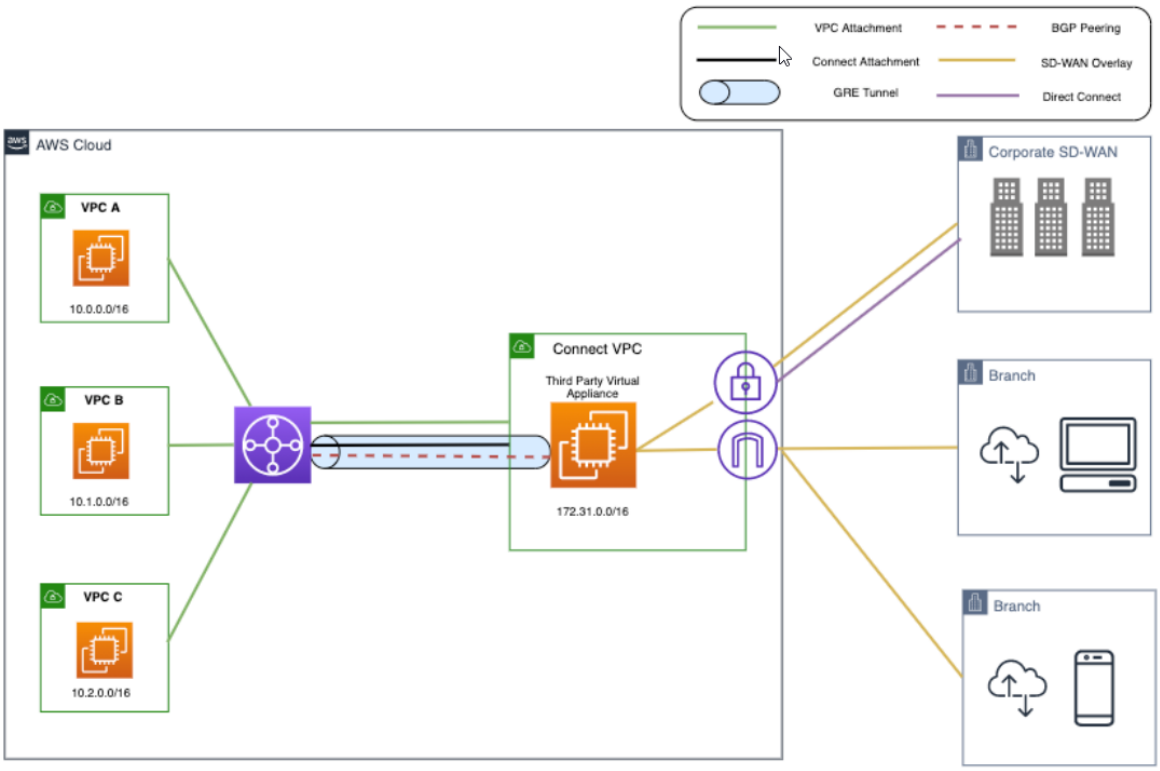


Figure 1 Q21 AWS transit Gateway

Option A is incorrect. Using IPsec between SD-WAN appliance and AWS Transit Gateway will incur additional operational overhead. Using AWS Transit Gateway Connect Attachment can provide better performance in a simpler way. **Option B is incorrect.** The GRE tunnel cannot be created directly to AWS Transit Gateway. It requires a Transit Gateway Connect attachment for the GRE tunnel. **Option D is incorrect.** AWS Transit gateway connect attachments support GRE Tunnel and not IPsec tunnel.

For more information on connecting SD-WAN infrastructure to AWS, refer to the following URL,https://aws.amazon.com/blogs/networking-and-content-delivery/simplify-sd-wan-connectivity-with-aws-transit-gateway-connect/

Domain: Network Design

22. A global oil company has a head office & data centre in New York while branch offices are in Tokyo and Sydney. The company is looking to move some of the applications to the AWS cloud. For application traffic between data centers & AWS, they are looking for a bandwidth capacity of 10 Gbps. At branch locations, 500Mbps bandwidth will be required. Communication should be enabled between the Branch office to Data Centre, Branch Office to AWS VPC in all regions. Communication should not be established between branch offices. Traffic should preferably ride on the AWS backbone for inter-region communication. All the connectivity should be fully resilient.

What of the following designs can be recommended to meet these requirements?

A> Create 2x 10Gbps AWS Direct Connect Links between data center & AWS using AWS Transit Gateway. Create managed Site-to-Site VPN from branch office to virtual transit gateway attached to VPC in respective AWS regions. Create Transit Gateway peering between transit gateway in each region. Configure BGP route propagation at each transit gateway in different regions for routing traffic between regions. Configure Transit Gateway route tables to deny communication between branch offices.

B> Create 2x 10Gbps AWS Direct Connect Links between data center & AWS using AWS virtual private gateway. Create managed Site-to-Site VPN from branch office to virtual private gateway attached to VPC in respective AWS regions. Implement VPC to VPC connectivity using AWS transit gateway in each region. Configure Static routes at each transit gateway in different regions for routing traffic between regions. Configure Transit Gateway route tables to deny communication between branch offices.

C> c. Create Accelerated Site-to-Site VPN between data center & AWS using AWS Transit Gateway. Create Accelerated Site-to-Site VPN from branch office to nearest AWS edge location in respective AWS regions. Create Transit Gateway peering between transit gateway in each region. Configure BGP route propagation at each transit gateway in different regions for routing traffic between regions. Configure Transit Gateway route tables to deny communication between branch offices.

D> Create 2x 10Gbps AWS Direct Connect Links between data center & AWS using AWS Transit Gateway. Create Accelerated Site-to-Site VPN from branch office to nearest AWS edge location in respective AWS regions. Create Transit Gateway peering between transit gateway in each region. Configure Static routes at each transit gateway in different regions for routing traffic between regions. Configure Transit Gateway route tables to deny communication between branch offices.

Explanation:

Correct Answer: D

For establishing connectivity as per requirement, the following can be designed,

1. *Create 2x 10Gbps AWS Direct Connect Links between data center & AWS using AWS Transit Gateway: This will provide high-performance consistent connectivity from datacenter to AWS. 2x 10 Gbps links will provide redundant connectivity.*
2. *Create Accelerated Site-to-Site VPN from branch office to nearest AWS edge location in respective AWS regions: With Accelerated Site-to-Site VPN, customer router establishes an IPsec VPN to nearest AWS edge location. This ensures traffic utilizes AWS global network for inter-region communication. Accelerated Site-to- Site VPN provides optimal latency for inter-region traffic as compared to AWS Site-to-Site VPN.*
3. *Create Transit Gateway by peering between transit gateway in each region: This will provide communication between two regions.*
4. *Configure Static routes at each transit gateway in different regions for routing traffic between regions: Static routes are required since BGP route propagation is not supported for Transit Gateway inter-region peering.*
5. *Transit gateway routing can be configured to deny communications between branch offices.*

Option A is incorrect as all traffic for Site-to-Site managed VPN will be flowing over the internet end-to-end from customer location to transit gateway. This VPN will not use AWS global network for traffic flow.

Option B is incorrect as all traffic for Site-to-Site managed VPN will be flowing over the internet end-to-end from customer location to transit gateway. This VPN will not use AWS global network for traffic flow.

Option C is incorrect as BGP route propagation is not supported between AWS Transit gateways in different regions.

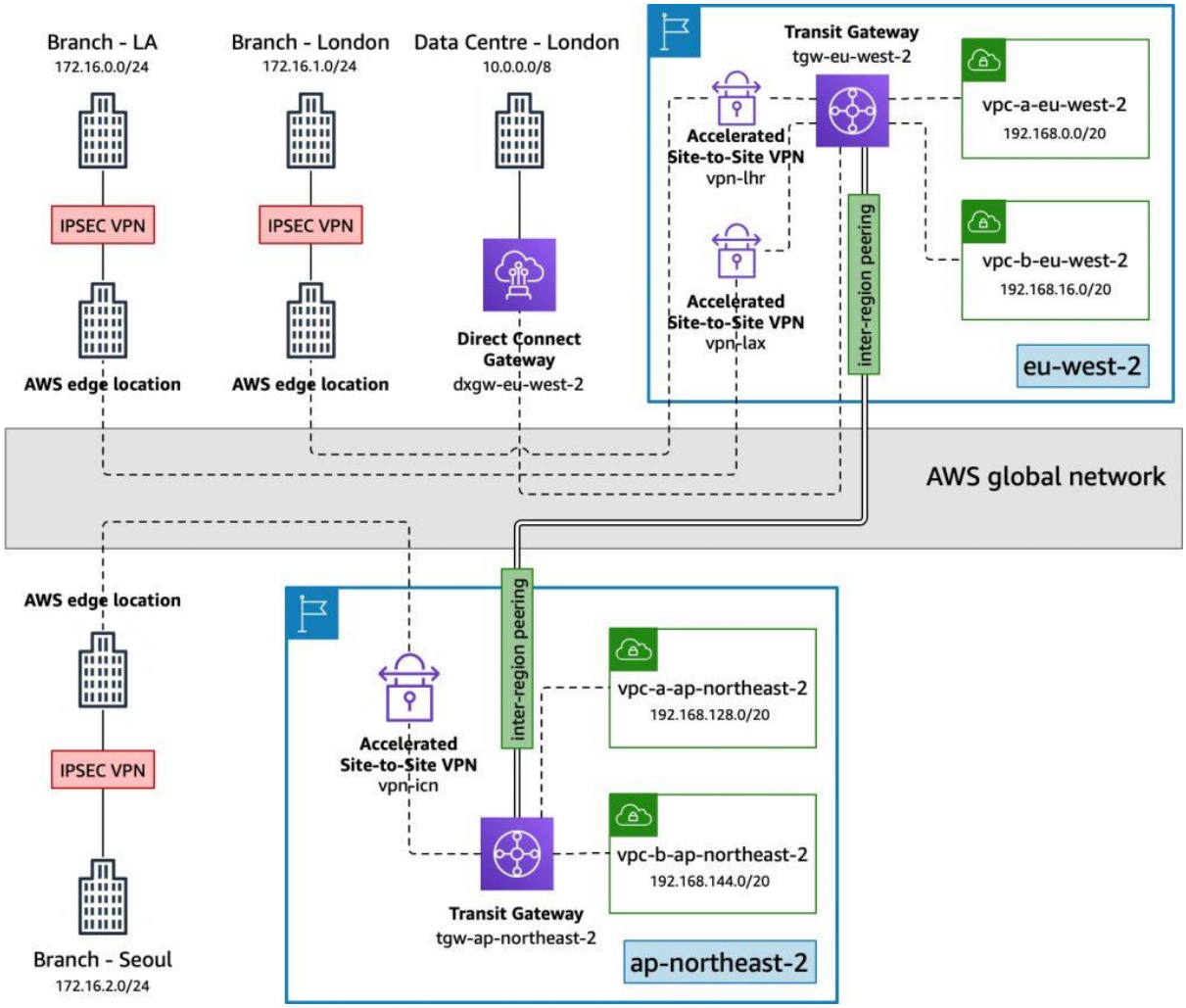


Figure 2 Network Design

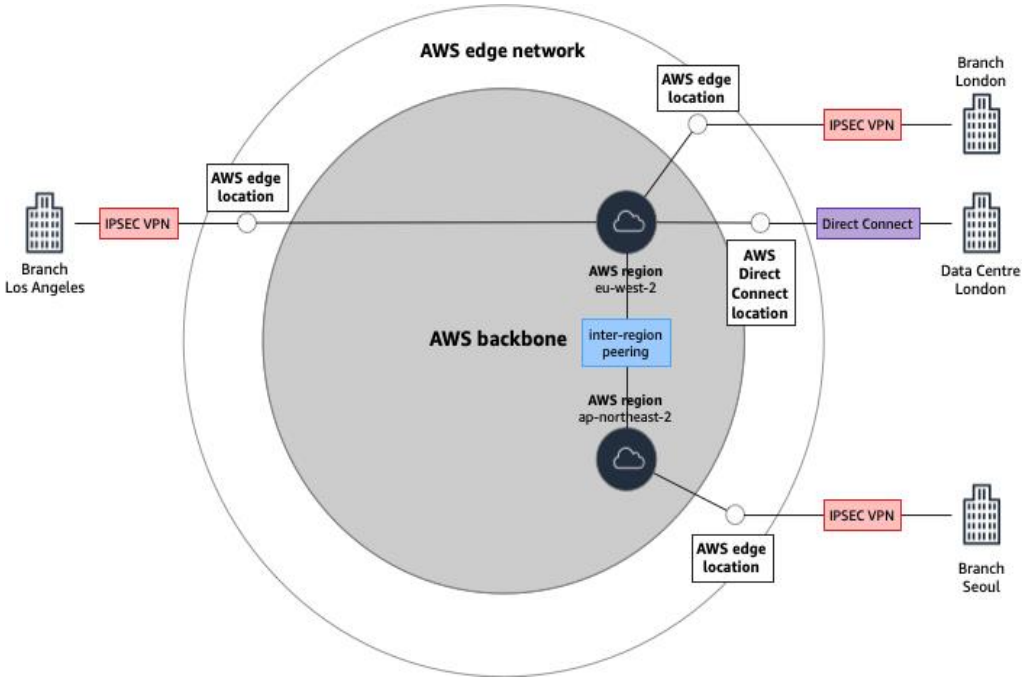


Figure 3 AWS Transit Gateways are peered with one another

For more information on Accelerated Site-to-Site VPN and Transit Gateway peering, refer to the following URLS,

https://docs.aws.amazon.com/vpc/latest/tgw/tgw-peering.html

https://aws.amazon.com/blogs/networking-and-content-delivery/building-a-global-network-using-aws-transit-gateway-inter-region-peering/

Domain: Network Implementation

23. An IT firm has deployed three VPCs as VPC A, VPC B, & VPC C. All internet traffic should be forwarded via VPC C. Two subnets are created in VPC C, a private subnet, and a public subnet. NAT Gateway & an Internet Gateway are deployed in the public subnet of VPC C. All VPC A, B, and C are inter-connected via AWS Transit Gateway using private subnets of each VPC. How should routing be configured for VPC A, VPC B, and the Transit gateway to forward all internet traffic via VPC C?

A> In VPC A and VPC B, add a default route pointing to the Transit Gateway. In Transit Gateway, create a static default 0.0.0.0/0 pointing to NAT Gateway.
B> In VPC A and VPC B, add a default route pointing to the Transit Gateway. In the Transit Gateway, the

C> In VPC A and VPC B, add a default route pointing to NAT Gateway. In Transit Gateway, create a static default 0.0.0.0/0 pointing to the public subnet of VPC C.

D> **In VPC A and VPC B, add a default route pointing to Transit Gateway. In Transit Gateway, create a static default 0.0.0.0/0 pointing to VPC C Attachment.**

Correct Answer: D

AWS Transit Gateway can be implemented to route outbound internet traffic to a VPC having an Internet gateway from VPC without an Internet Gateway. For this configuration in VPC A & VPC B which have an Internet Gateway, a default route is added pointing to Transit Gateway. In the transit gateway, a static default route is added pointing to the VPC C attachment. This will forward all internet traffic from VPC A & VPC C to VPC C. VPC C will forward traffic to the internet using the NAT gateway and Internet gateway.

Connectivity will be as follows:

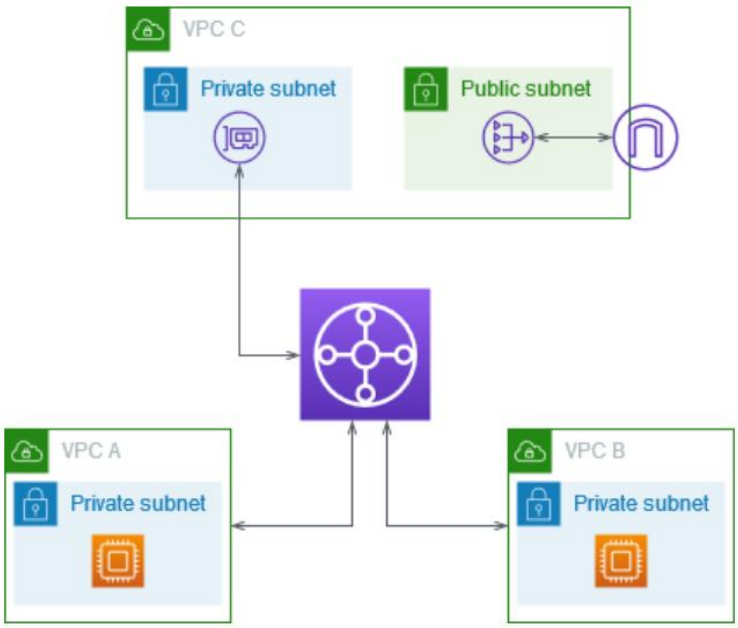


Figure 4 Q23

Option A is incorrect as in Transit Gateway Default route should be added pointing towards VPC C attachments and not to NAT Gateway.

Option B is incorrect as in Transit Gateway Default route would not be propagated directly via VPC attachment for VPC C. A static default must be added in Transit Gateway to forward internet traffic to VPC C.

Option C is incorrect as in VPC A and VPC B default route should be pointing to Transit Gateway and not to NAT Gateway. In the Transit Gateway Default route should be added pointing towards VPC C attachments and not to the public subnet of VPC C.

For more information on using Transit gateway to route outbound internet traffic, refer to the following URL,

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-nat-igw.html

Domain: Network Security, Compliance, and Governance

24. A cloud-based company has created a service provider VPC to share applications with another customer VPC. In Service provider VPC, the application is deployed on Amazon EC2 instance with an Application Load balancer as a front end for load balancing incoming traffic. In customer VPC, a host-based firewall is configured on all Amazon EC2 instances which needs to allow a destination IP pool to complete communication with the application in service provider VPC.

How settings can be configured to ensure communication between the EC2 instance and the application?

A> In Firewall, allow IP range for Application Load Balancer matching IP pool for the entire Availability Zone.
B> Manually update the IP address of the Application Load Balancer in the firewall.
C> Deploy a Network Load Balancer in service provider VPC. Use the Application Load Balancer as a target for Network Load Balancer. Use the Static IP address of the Network Load Balancer to create rules in Firewall.
D> Use AWS Lambda functions to enable static IP addresses for Application Load Balancer.

Explanation:

Correct Answer: C

Application Load Balancer IP addresses are dynamic and change while scaling. The Application Load balancer can be used used as a target for the Network load balancer. A static NLB IP address for the Application Load balancer will help in allowing this static IP in the firewall rules. This eliminates the need to manually configure firewall rules or use any additional codes to modify firewall rules when the Application load balancer IP address changes.

Option A is incorrect as allowing a longer IP pool is against security best practices. **Option B is incorrect** as manually updating the IP address of the Application Load balancer in the firewall will lead to additional configuration changes when there is a change in the IP address of the application load balancer. **Option D is incorrect** as AWS Lambda functions can be used. This will incur additional coding & management efforts.

For more information on using Application Load Balancer as a target for Network Load Balancer, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/application-load-balancer-type-target-group-for-network-load-balancer/

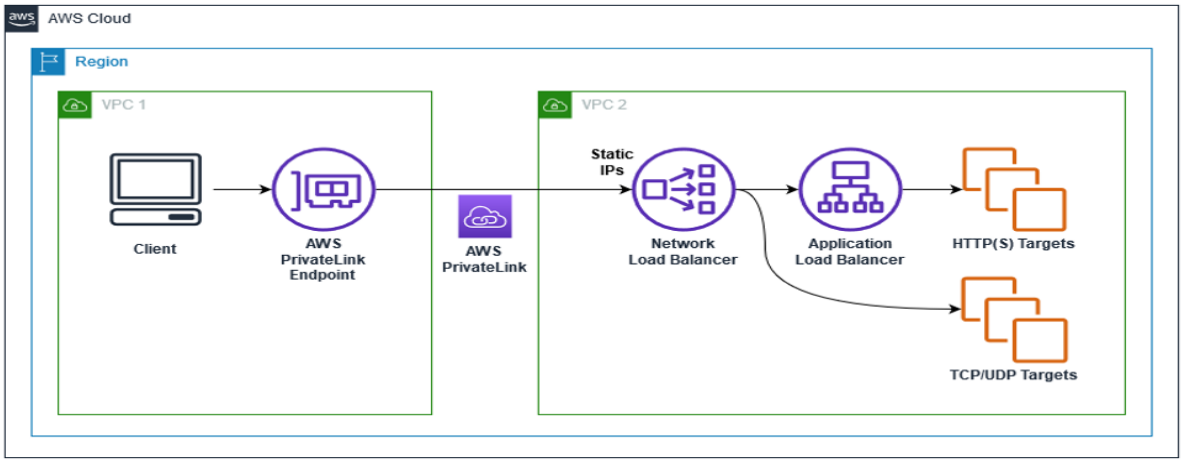


Figure 1: Q24-1 ALB as a Target of NLB high level architecture diagram. Use Cases – PrivateLink, Static IP & Multi-Protocol Connections

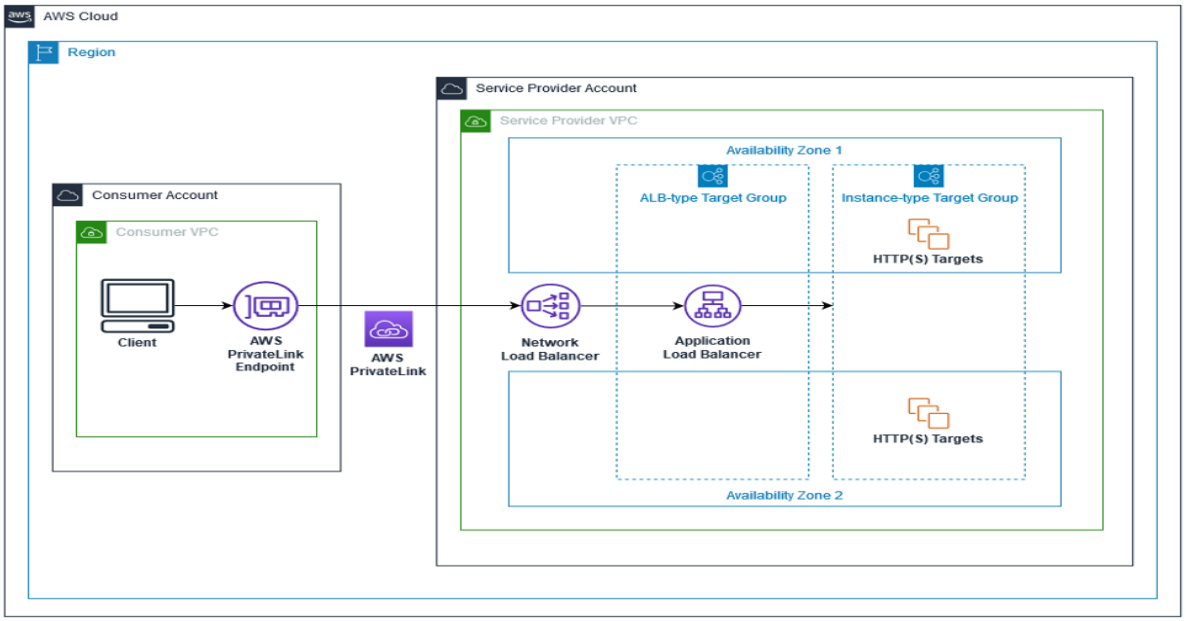


Figure 2: Q24-2 ALB as a Target of NLB detailed architecture diagram – Private Link Use Case

Domain: Network Implementation

25. A start-up firm plans to deploy Application Load Balancer to distribute incoming traffic to multiple Amazon EC2 instance hosting applications. Amazon EC2 instances are configured in a group that has an application configured that caters to specific users based upon the source location. The firm is looking for

your guidance in setting up Application Load Balancer to forward traffic from users to specific Amazon EC2 instances.

What suggestion can be provided to forward traffic to EC2 targets conditionally?

A> Create a listener rule with a condition rule matching host-header.
B> Create a listener rule with a condition rule matching http-header.
C> Create a listener rule with a condition rule matching source-ip.
D> Create a listener rule with a condition rule matching the X-Forwarded-For header.

Explanation:

Correct Answer: B

Following conditions types are supported for creating rules,

1. *host-header: Route based on the host name of each request.*
2. *http-header: Route based on the HTTP headers for each request.*
3. *http-request-method: Route based on the HTTP request method of each request.*
4. *path-pattern: Route based on path patterns in the request URLs.*
5. *Query-string: Route based on key/value pairs or values in the query strings.*
6. *source-ip: Route based on the source IP address of each request.*

X-Forwarded-For header source-ip condition does not match the IP address in the X-Forwarded-For header. To create a rule based upon the IP address in the X-Forwarded-For header, the http-header must be used while creating a conditional rule.

Option A is incorrect as the matching host header will not match the IP address of the client.

Option C is incorrect. For matching addresses within the X-Forwarded-For header, the source-ip header cannot be used. The http-header needs to be used to search IP addresses within the X-Forwarded-For header.

Option D is incorrect as the X-Forwarded-For header is not a valid header for matching with the condition rule. The http-header needs to be used to search IP addresses within the X-Forwarded-For header.

For more information on creating listener rules with Application Load Balancer, refer to the following URL,

https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-listeners.html

26. A Software as a service provider (SaaS) has created a service provider VPC for sharing Amazon Kinesis Data Streams.

Users from Customer VPC connect to this service using AWS PrivateLink. To access Kinesis Data Streams, sustained high throughput of 20Gbps is required from each Availability zone.

How can the AWS PrivateLink interface be designed to meet throughput requirements?

A>Create two interface endpoints using AWS Private link with Private DNS disabled. Create a Private hosted zone in Amazon Route 53 for Kinesis Data Streams and associate it with Consumer VPC. Create a weighted route policy with Alias A records pointing to interface endpoints to distribute traffic on both interface endpoints.

B> Create two interface endpoints using AWS Private link with Private DNS enabled. Create a Private hosted zone in Amazon Route 53 for Kinesis Data Streams and associate it with Consumer VPC. Create a weighted route policy with Alias A records pointing to interface endpoints to distribute traffic on both interface endpoints.

C> Create two interface endpoints using AWS Private link with Private DNS disabled. Create a Private hosted zone in Amazon Route 53 for Kinesis Data Streams and associate it with Consumer VPC. Create a multivalue answer route policy with Alias A records pointing to interface endpoints to distribute traffic on both interface endpoints.

D> Create two interface endpoints using AWS Private link with Private DNS enabled. Create a Private hosted zone in Amazon Route 53 for Kinesis Data Streams and associate it with Consumer VPC. Create a weighted route policy with CNAME A records pointing to interface endpoints to distribute traffic on both interface endpoints.

Explanation:

Correct Answer: A

Interface Endpoint supports bandwidth up to 10 Gbps with bursts up to 40Gbps. To get sustained bandwidth above 10Gbps following design can be considered,

I. *Create Multiple interface endpoints from each Availability zone: This will help to increase total bandwidth between consumer VPC and service provider VPC.*
II. *Set PrivateDNSEnabled as False for these interfaces: Private DNS associated with interface endpoints do not support multiple interface endpoints.*
III. *Create a Private Hosted zone in Route53 for the service in service provider VPC and attached to the consumer VPC.*

IV. Create weighted Alias A records for DNS names of the interface endpoints: This will help distribute traffic across multiple interface endpoints.

Option B is incorrect. Private DNS should be disabled as it does not support traffic over multiple interface endpoints.

Option C is incorrect. To distribute traffic over multiple interface endpoints, the routing policy should be a weighted routing policy, not a multivalue answer route policy. With a multivalue answer route policy, end-users may send traffic to any one of the DNS hosts.

Option D is incorrect as the Alias record should be created, not the CNAME.

For more information on higher bandwidth while using AWS PrivateLink, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/scale-traffic-using-multiple-interface-endpoints/

Domain: Network Design

27. A media company plans to store on-premises data to Amazon S3 for backup purposes using Amazon S3 File Gateway. A large amount of data would be transferred from on-premises regularly. Optimal Latency is required for this data transfer. IT Team is looking for scalable and fully resilient connectivity for this data transfer from an on-premises file gateway to Amazon S3.

What connectivity can be designed for this purpose?

A>Setup an S3 interface endpoint from VPC private subnet. Connect Amazon S3 File Gateway using this interface endpoint to Amazon S3 over AWS Direct Connect links.

B> Setup an HTTP proxy Amazon EC2 instance in a VPC private subnet. Configure the S3 gateway endpoint in this VPC. Use this proxy infrastructure to pass all traffic from Amazon S3 File Gateway to Amazon S3 over AWS Direct Connect links.

C> Setup Site-to-Site VPN to the virtual private gateway over an internet link. Use this VPN to pass all traffic from Amazon S3 File Gateway to Amazon S3.

D> Setup VPN to Amazon EC2 instance over internet link using third-party software VPN. Configure the S3 gateway endpoint in this VPC. Use this VPN to pass all traffic from Amazon S3 File Gateway to Amazon S3.

Explanation:

Correct Answer: A

Amazon S3 File Gateway can be used to store on-premises application data to Amazon S3. AWS PrivateLink can be used to create private connectivity between Amazon VPC and AWS services. From On-premises, connectivity is established with AWS using either AWS Direct Connect or AWS Site-to-Site VPN. Over this connectivity, the Amazon S3 file gateway can connect to the Amazon S3 bucket via AWS PrivateLink.

S3 interface endpoint is created in a VPC to have private connectivity with Amazon S3. AWS S3 File gateway appliance in the on-premises location connects to the $3 interface endpoint and then establishes connectivity with the Amazon S3 bucket. Since connectivity is private between VPC and S3 buckets, an optimal latency is obtained. Each Interface endpoint supports up to 10Gbps of bandwidth. Additional Interface endpoints can be created for bandwidth requirements above 10Gbps. Dual AWS Direct Connect links can be added for resiliency.

The connectivity Diagram will be as follows.

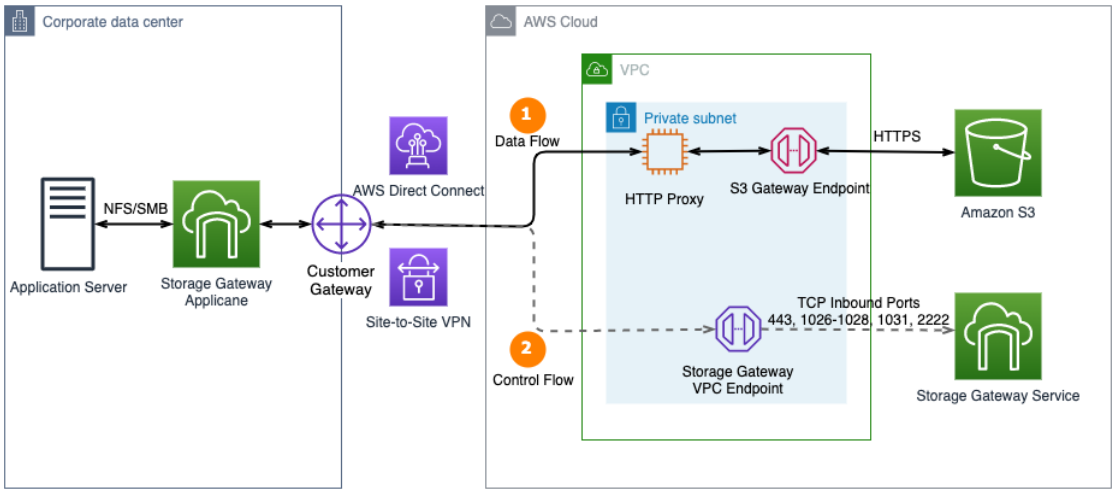


Figure 1. Connect to Amazon S3 Gateway endpoint using an HTTP proxy

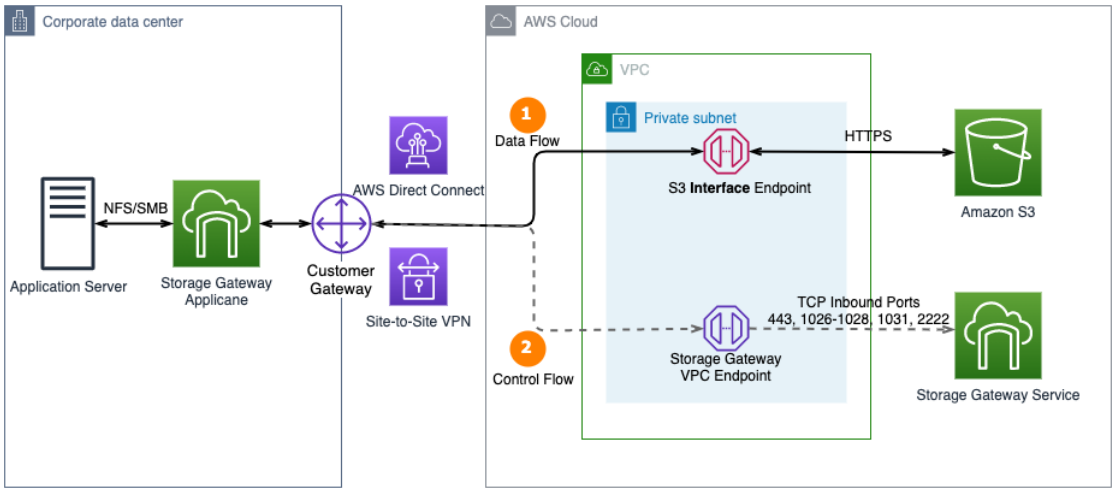


Figure 2. AWS Storage Gateway now supports AWS PrivateLink for Amazon S3 endpoints and Amazon S3 Access Points

Option B is incorrect. Although this will work, this will lead to additional configuration and operational overhead.

Option C is incorrect. For Site-to-Site VPN using a Virtual private gateway, there is a bandwidth limitation of 1.25Gbps. This will lead to bandwidth constraints for large data transfers.

Option D is incorrect. This will not be a scalable solution. Also, additional configuration will be needed to have a failover for the Amazon EC2 instance on which VPN is terminated.

https://aws.amazon.com/blogs/architecture/connect-amazon-s3-file-gateway-using-aws-privatelink-for-amazon-s3/

Domain: Network Implementation

28. A start-up company plans to connect three of its locations to AWS Cloud using AWS Site-to-Site VPN. This connectivity will be established using existing internet connections. All three locations need to communicate with the VPCs having subnets in multiple AZs. Additionally, all three locations need to communicate with each other. The company is planning to set up AWS Direct Connect at one of the locations in the near future; the proposed solution should be feasible for this connectivity as well.

How can connectivity be built to meet this requirement?

A> Create customer gateways with the same BGP ASN at each customer location. Create a Site-to-Site VPN with dynamic routing Protocol BGP to a different VGW attached to a separate VPC. Create VPC peering between these VPCs. Configure the customer gateway devices to advertise a site-specific prefix to the VGW.

B> Create customer gateways with unique BGP ASN at each customer location. Create a Site- to-Site VPN with dynamic routing protocol BGP to a common VGW. Configure the customer gateway devices to advertise a site-specific prefix to the VGW.

C> Create customer gateways with the same BGP ASN at each customer location. Create a Site-to-Site VPN with dynamic routing protocol BGP to a common VGW. Configure the customer gateway devices to advertise a default prefix to the VGW.

D> Create customer gateways with unique BGP ASN at each customer gateway. Create a Site- to-Site VPN with dynamic routing protocol BGP to a different VGW attached to a separate VPC. Create VPC peering between these VPCs. Configure the customer gateway devices to advertise a default prefix to the VGW.

Explanation:

Correct Answer: B

For *connecting multiple locations to the AWS cloud using AWS Site-to-Site VPN,*

1. Create a single Virtual Gateway and attach it to an AWS VPC.

2. Create a customer gateway at each of the customer locations. BGP ASN should be unique at each of the locations. A public IP address should be assigned to this gateway for creating VPN to VGW.

3. From each of the customer gateway, a site-specific prefix needs to be advertised to the VGW.

4. At VGW, route propagation can enable subnets in VPC to communicate with subnets at multiple sites.

5. AWS VPN Cloud Hub can provide communication between customer sites if one of the sites is connecting to VGW on AWS Direct Connect.

The following diagram shows connectivity between AWS VPN Cloud Hub

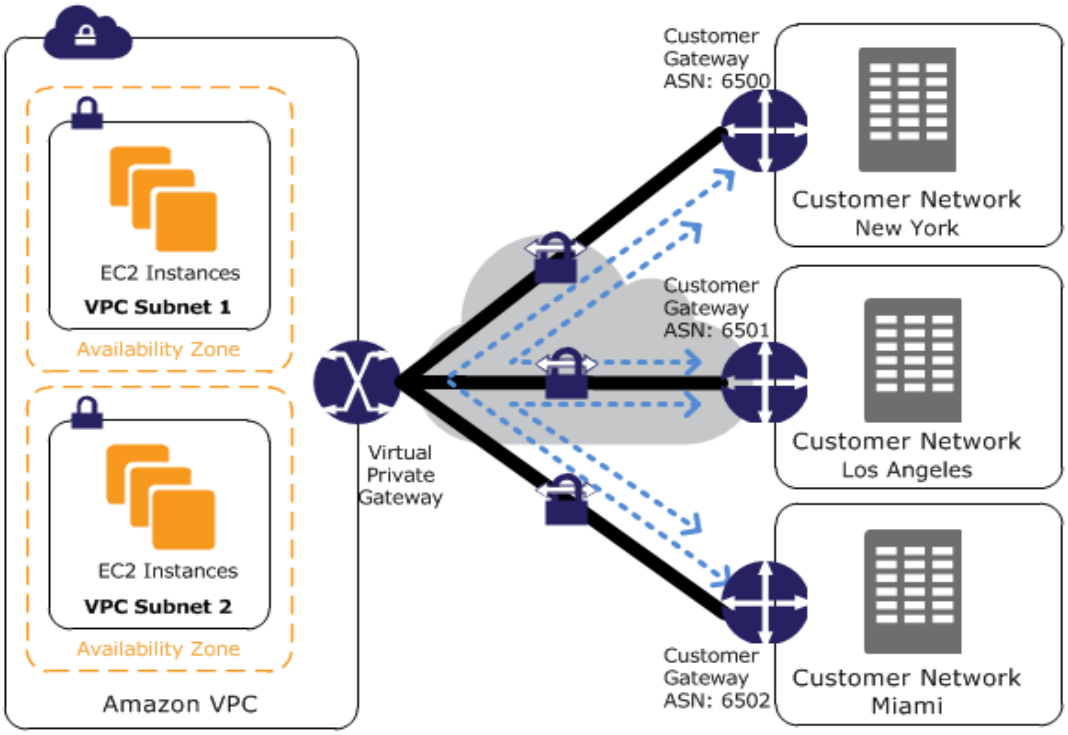


Figure 5 Q28 connect three of its locations to AWS Cloud using AWS Site-to-Site VPN

Option A is incorrect. BGP ASN for each customer site should be unique. Also, with VPC peering, transitive routing is not allowed. Sites connecting to different VPCs cannot communicate with each other over VPC peering.

Option C is incorrect. BGP ASN for each customer site should be unique. Customer Gateway devices should advertise a site-specific prefix to the AWS VGW, not a default route.

Option D is incorrect. The Customer Gateway device should advertise a site-specific prefix to the AWS VGW, not a default route. Also, with VPC peering, transitive routing is not allowed. Sites connecting to different VPCs cannot communicate with each other over VPC peering.

Domain: Network Security, Compliance, and Governance

29. A pharma company is deploying multiple web servers on EC2 instances in multiple VPCs. The security team has provided separate IP pools and TCP ports to reach each of these web servers based on the servers' functions and their access requirements. The security team needs a standard solution to allow and block some of these TCP ports for their current and future deployments. Which of the following options can be used to meet this requirement?

A> Create separate Security Groups for each instance & assign them to each instance. Use NACL to deny TCP ports to all instances at the subnet level.

B> Launch an instance in separate subnet & apply separate NACL to each instance. Use Security Groups to deny TCP ports to all instances.

C> Create separate Security Groups for each instance & assign them to each instance. Use Security Groups to deny TCP ports to all instances in all subnets.

D> Launch an instance in a separate subnet & apply separate NACL to each instance. Use NACL to deny TCP ports to all instances.

Explanation:

Correct Answer - A

NACL can be used at the subnet level to block or allow IP / Ports. Security Groups can be used at the instance level to allow a specific IP address or ports to the instance. Security Groups cannot be used to deny traffic. In the above, since all the servers have different IP Pools & Ports to be allowed, Security Groups can be used per server instance. NACL can be used to deny all unwanted ports which will be applied at the subnet level & will apply to all server instances in that subnet.

Options B & C are incorrect as Security Groups cannot be used to deny traffic. Option D is incorrect as Launching an instance in a separate subnet is not a feasible option.

For more information on using Security Groups & NACL, refer to the following URLS

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

Domain: Network Implementation

30. A global IT firm has deployed the company's website on EC2 instance behind ELB. AWS CloudFront is configured with origin as ELB to serve all web content with the lowest latency to global partners. A Security Group is configured on ELB to ensure only AWS CloudFront IP ranges can access ELB & web content hosted on EC2 instance. Recently there were changes in AWS CloudFront IP ranges that were not allowed in Security Groups impacting partner access to the website. Which of the following tasks can be executed with minimum efforts & cost to update Security Groups attached to ELB to allow only valid AWS CloudFront IP Pool associated with Security Groups?

A. Create a Lambda function based upon VPC flow logs, which will automatically check if any IP ranges apart from CloudFront IP pools are reaching ELB & modify Security Groups automatically.

B. Create a cron job to poll VPC flow logs which will check if any IP ranges apart from CloudFront IP pools are reaching ELB & modify Security Groups accordingly.

C. Create a Lambda function based upon AWS SNS trigger for change in AWS CloudFront IP ranges to update Security Groups attached to ELB automatically.

D. Create a cron job to poll CloudFront IP ranges to verify any changes & manually modify Security Groups attached to ELB if any change in IP ranges.

Explanation:

Correct Answer - C

When an AWS CloudFront IP ranges are updated, an AWS SNS topic is generated. To automatically update Security Groups attached to ELB, a Lambda function can be created which is triggered for AWS SNS topic & in turn update Security Groups to only allow those updated IP ranges to access origin ELB. This is cost-effective as the Lambda function is triggered only when an AWS SNS topic for AWS IP range changes is added.

Option A is incorrect as this will not proactively update IP pool changes in Security Groups.

Options B & D are incorrect as this will need to modify Security Groups manually each time there is a change in AWS CloudFront IP ranges.

For more information on updating Security Groups automatically, refer to the following URL

https://aws.amazon.com/blogs/security/how-to-automatically-update-your-security-groups-for-amazon-cloudfront-and-aws-waf-by-using-aws-lambda/

Domain: Network Security, Compliance, and Governance

31. A global airline company has set up multiple VPCs in multiple regions for its three-tier application which is used for ticketing purposes by agents. Recently the IT team of this company has developed a new ticketing application which they need to evaluate on the test setup. For this, a new TEST VPC needs to be created & EC2 instances with the new applications need to be launched in this VPC. A Junior Engineer who was responsible for implementing this new setup did not specify Security Groups on all-new EC2 instances launched within TEST VPC. How will this impact communication between instances in TEST VPC?

A>Will allow all inbound traffic from instance within the same Security Groups & will allow all outbound traffic from the instance.

B> Will deny all inbound & outbound traffic from each instance.

C> Will allow all outbound traffic from instance within the same Security Groups & will allow all inbound traffic from the instance.
D> Will permit all inbound & outbound traffic between instances.

Explanation:

Correct Answer - A

When no Security Groups are specified during launch, the instance will be launched in default Security Groups for that VPC. In the case of default Security Groups, it will allow all inbound traffic from all instances with that Security Groups & allow all outbound traffic from the instance.

Option B is incorrect as with no Security Groups specified, a default Security Groups will be applied which do not deny all inbound & outbound traffic but all inbound traffic from instance within the same Security Groups & allows all outbound traffic.

Option C is incorrect as Default Security Groups allow all outbound traffic irrespective of the same Security Groups & do not allow all inbound traffic.

Option D is incorrect as for inbound traffic default Security Groups will allow traffic from an instance with the same Security Groups & will deny all other traffic.

For more information on using Default Security Groups, refer to the following URLS,

https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html

Practice Test-1 Question 11 Of 65

Domain: Network Implementation

32. An online grocery store has deployed a new application using Amazon RDS as a database. Developers located at on- premises need to access RDS DB instances. Due to a limited budget, they will be using existing internet links for connection to the AWS cloud. Security Head is seeking your advice to develop a security solution for this remote access. Also, the solution needs to be scalable.

Which of the following is the most secure way of accessing the Amazon RDS instance from the on-premises location?

A> Create a publicly accessible Amazon EC2 instance. Access EC2 instance using Site-to-Site VPN created over IPsec using VGW. Login to this instance from an on-premises location and then access the RDS instance in a private DB subnet.

B> Create a publicly accessible RDS instance. Attach a network ACL to DB subnet, allowing only subnet from on-premises & deny all other prefixes. Access RDS instance using the internet at the on-premises location.

C> Create an AWS Client VPN. Deploy the RDS instance in a private subnet in the VPC. Associate DB instance subnet with AWS Client VPN interface endpoint.

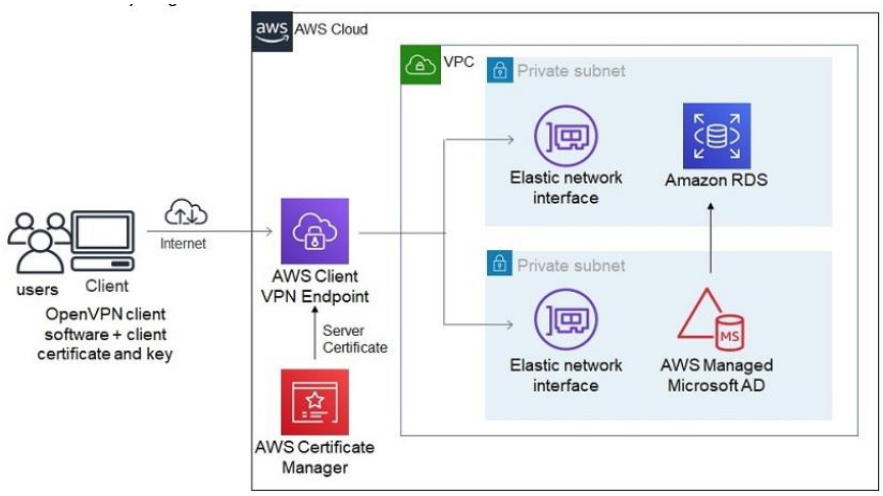
D> Create a publicly accessible Amazon EC2 instance. Access EC2 instance using public IP address over the internet. Login to this instance from an on-premises location and then access the RDS instance in a private DB subnet.

Explanation:

Correct Answer: C

AWS Client VPN is a managed solution that can help establish secure connectivity from users to AWS services. The client establishes a secure VPN connection using OpenVPN software which terminates on the AWS client VPN endpoint. AWS services that need to be accessed remotely are associated with this AWS client VPN endpoint. In the above scenario, an RDS instance is launched in a VPC private subnet. This subnet is associated with the AWS Client VPN endpoint. AWS Client VPN provides a scalable option for connecting to any AWS resources from an on-premises location.

The connectivity diagram will be as follows,



Option A is incorrect. This is a sub-optimal way of accessing the Amazon RDS instance. Using AWS Client VPN is a better option for accessing RDS instances remotely.

Option B is incorrect. This will require RDS instances to be placed in public subnets which increases security risk.

Option D is incorrect. This is not a secure way of accessing RDS instances.

For more information on accessing RDS instance remotely, refer to the following URL,

https://aws.amazon.com/blogs/database/accessing-an-amazon-rds-instance-remotely-using-aws-client-vpn/

Domain: Network Design

34. You are working as an AWS Consultant for a global IT company. The company has deployed its application in AWS Cloud across two regions. VPC peering is already configured between VPCs in these two regions. The company has deployed AWS Managed Microsoft Active Directory (AD) in these regions with multi-region replication configured between them. All global remote users need to be authenticated by this active directory before accessing applications in VPC. The company wants to build secure connectivity having optimal latency between global remote users and the active directory. A fully fault-tolerant and scalable solution should be deployed.

What design can be proposed to meet the requirement?

A> Configure all remote users to use bastion hosts deployed at the on-premises location. Create a managed Site-To-Site VPN from an on-premises location to AWS using AWS Transit Gateway. Associate VPC with AWS Managed Microsoft AD with AWS Transit Gateway at each region. Configure peering between AWS Transit Gateway at each region.

B> Deploy a third-party software VPN in the Amazon EC2 instance in the same VPC as that of the active directory. Remote users will use an open-source VPN to connect to Amazon EC2 instances and then will be authenticated via Associate AWS Managed Microsoft AD.

C> Create a Client VPN endpoint in both regions. Associate AWS Managed Microsoft AD instance with client VPN endpoints in both regions. Share Client VPN configuration files to users based upon geographically nearest region.

D> Create a Client VPN endpoint in both regions. Associate AWS Managed Microsoft AD instance with client VPN endpoints in both regions. Create a Route53 public-hosted zone. Create CNAME records pointing to the DNS name of the endpoint with latency-based routing and health checks.

Explanation:

Correct Answer: D

AWS Client VPN provides a secure managed VPN connectivity between users and AWS services. With public hosted zones created in Route 53 pointing to client VPN interfaces based on latency-based routing, remote users will be pointed to client VPN interfaces with optimal latency.

AWS Managed Microsoft AD can be associated with the client VPN interface, which remote users can use for authentication.

The connectivity diagram is as follows,

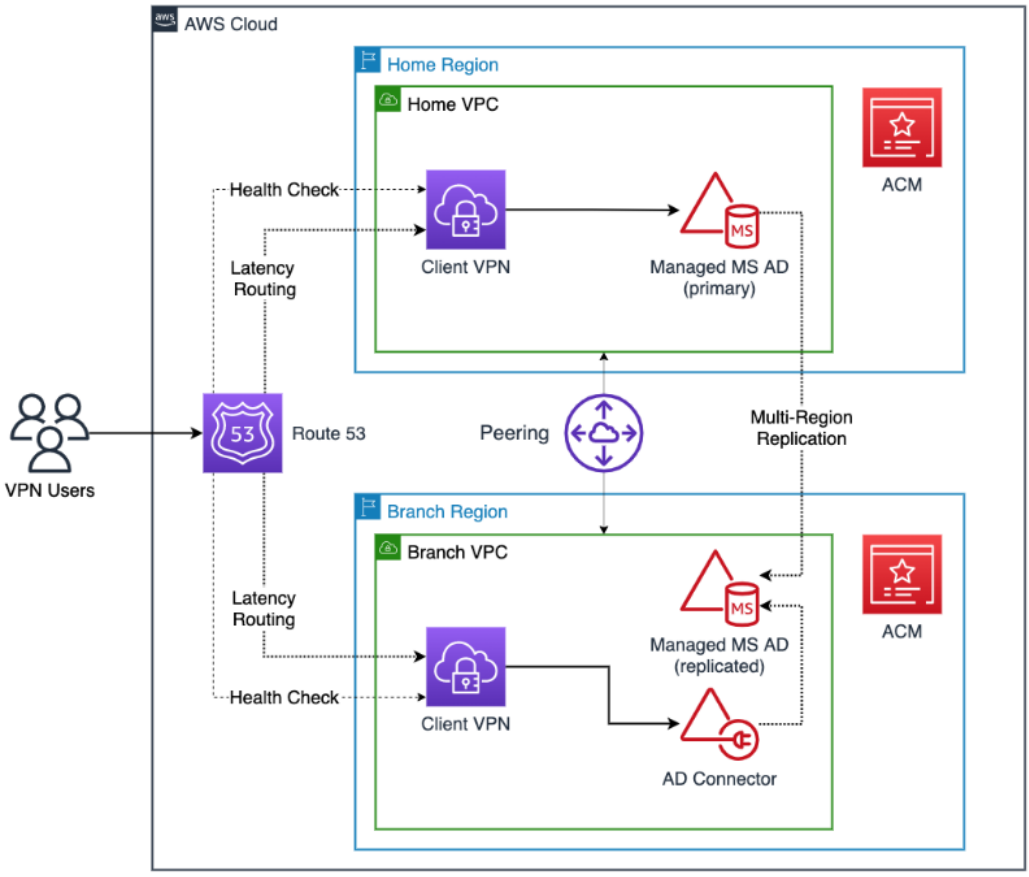


Figure 6 Q 34 AWS Managed Microsoft AD can be associated with the client VPN interface

Option A is incorrect. Using bastion host and site-to-site VPN is not a scalable solution. This will also incur high latency for all remote users to first connect to on-premises location and from there initiate connectivity to AWS Managed Microsoft AD. **Option B is incorrect**. This solution will not be scalable. Building resiliency with Amazon EC2 instances across two regions will incur additional admin work. **Option C is incorrect** as Sharing Client VPN configuration files with the geographically nearest location will not guarantee optimal latency between users and the active directory.

For more information on using Route 53 along with Client VPN for multi-region connectivity, refer to the following URLS,

https://aws.amazon.com/blogs/networking-and-content-delivery/building-multi-region-aws-client-vpn-with-microsoft-active-directory-and-amazon-route-53/

35. An IT company has created a private hosted zone for a new application launched in VPC A. This application will be accessed from a large number of VPCs across multiple regions. The quality assurance team is looking for the DNS queries made

while accessing this application in real-time to troubleshoot application issues related to the DNS.

What can be configured to meet this requirement?

A> Configure Route 53 Resolver Query Logs. Select destination for these logs as Amazon S3 bucket.
B> Configure Route 53 Public DNS Query Logs. Select the destination for these logs as Amazon CloudWatch Logs.
C> Configure Route 53 Public DNS Query Logs. Select the destination for these logs as Amazon Kinesis Data Firehose.
D> **Configure Route 53 Resolver Query Logs. Select the destination for these logs as Amazon Kinesis Data Firehose**.

Explanation:

Correct Answer: D

Route 53 Resolver Query Logs call DNS queries made by the resources within the VPC.

Destination for the DNS query logs can be one of the following

I. *Amazon CloudWatch Logs: To search, query, monitor metrics, or raise alarms based upon logs.*
II. *Amazon S3: For long-term storage of the logs for security compliance.*
III. *Amazon Kinesis Data Firehose: For real-time analysis of the DNS logs.*

Since the quality assurance team requires real-time analysis of the logs, the destination can be selected as Amazon Kinesis Data Firehose.

Option A is incorrect. As the client wants to analyse DNS queries in real-time, Amazon S3 is not an ideal destination for storing logs. **Option B is incorrect**. As the client wants to analyse DNS queries in real-time, Amazon CloudWatch Logs is not an ideal destination for storing logs. Route 53 Public DNS Query logs all DNS queries made from the internet and does not log queries made by resources within the VPC. Amazon CloudWatch Logs can be selected as a destination when there is a need to raise the alarm based upon DNS query logs. **Option C is incorrect** as Route 53 Public DNS Query logs all DNS queries made from the internet and does not log queries made by resources within the VPC.

For more information on Route 53 Resolver query logging, refer to the following URL,

https://aws.amazon.com/blogs/aws/log-your-vpc-dns-queries-with-route-53-resolver-query-logs/

Domain: Network Management and Operation

36. An engineering company uses hybrid connectivity between on-premises locations and the AWS cloud. The IT team has created a privately hosted zone example.com

and has associated with the VPC. They have also created an outbound Route53 resolver for example.com, and have related to this VPC. IT Team observes traffic routed to an on-premises network instead of routing based on records in a private hosted zone.

What could be the possible reason for such behaviour?

A> A public hosted zone needs to be created instead of a private hosted zone.
B> Amazon VPC has a private hosted zone that has enableDnsHostnames set to false.
C> Resolver rules will take precedence over private hosted zones.
D> Amazon VPC has a private hosted zone that has enableDnsSupport set to false.

Explanation:

Correct Answer: C

When a private hosted zone is created for a domain name and a resolver rule is created to route traffic to an on- premises network for the same domain name, traffic is routed based on resolver rules and not on records in the private hosted zones.

Option A is incorrect as only a private hosted zone needs to be created since queries will be within the VPC and not from the internet. **Option B is incorrect** as a private hosted zone can be created only if Amazon VPC has enableDnsHostnames enabled. **Option D is incorrect** as a private hosted zone cannot be created only if Amazon VPC has enableDnsSupport enabled.

For more information on Private hosted zones, refer to the following URL,

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zone-private-considerations.html

Domain: Network Management and Operation

37. A Sports Channel is broadcasting a major sports event. For this, the IT team has set up broadcasting using a multi- CDN architecture with Amazon CloudFront and a custom CDN deployed in Europe and Japan. This event will be viewed by viewers across the globe. Origin servers are deployed on Amazon EC2 instances in the us-east-1 region. The IT Team is observing an increase in load on origin servers during this event, due to which origin servers are intermittently becoming non-responsive. For future sports events, the IT team wants proactive measures to maintain the load on origin servers to acceptable levels.

What actions can be initiated to minimize load on origin servers?

A> Set up CloudFront Origin Shield in both Europe & Japan regions in front of custom CDN.
B> Set up CloudFront Origin Shield in the Regional cache location of the us-east-1 region.

C> Set up CloudFront Origin Shield in the Regional cache locations of Europe & Japan.
D> Set up CloudFront Origin Shield in edge cache locations of the us-east-1 region.

Explanation:

Correct Answer: B

Using multi-CDN architecture can increase the load on origin servers, as multiple requests from different edge locations or multiple regional cache locations need to be handled by the origin servers. To alleviate the load on origin servers, CloudFront Origin Shield can be deployed at one of the regional cache locations nearer to the Origin servers. With CloudFront Origin Shield, requests from other regional cache locations will not directly hit origin servers but will be directed to CloudFront Origin Shield.

In the above case, origin servers are deployed at the us-east-1 region, and CloudFront Origin Shield can be set up at the regional cache location in the us-east-1 region. This will minimize load on origin servers.

Option A is incorrect as CloudFront Origin Shield should be in a region closer to the origin server. Since origin servers are in the us-east-1 region, CloudFront Origin Shield should not be placed in Europe or Japan regions in front of custom CDN. **Option C is incorrect** as CloudFront Origin Shield should be in a region closer to the origin server. Since origin servers are in the us-east-1 region, CloudFront Origin Shield should be placed in Europe or Japan regions. **Option D is incorrect** as CloudFront Origin Shield should be placed at Regional Cache locations and not at edge locations.

For more information on CloudFront Origin Shield, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/using-cloudfront-origin-shield-to-protect-your-origin-in-a-multi-cdn-deployment/

Network Implementation

38. A government organization uses Amazon CloudFront to distribute content stored in Amazon EC2 instances. Some of this content is private & should not be cached at the CloudFront. When there is a viewer request for this private content, Amazon CloudFront should always retrieve this content from the Origin Amazon EC2 instance. For such content, the deployment team has added a header at the Origin as "Cache-Control: no-cache, no-store". It is observed that in some cases, when there is a request from viewers for this content and origin servers are not reachable, Amazon CloudFront is distributing cache copies.

What setting can be done at the Origin server end to avoid sharing cache copies from Amazon CloudFront?

A>At Origin, set headers as Cache-Control: stale-if-error=0
B> At Origin, set both headers, Cache-Control: max-age and Cache-Control: s-maxage
C> At Origin, add Expires header to the origin
D> At Origin, remove the header, Cache Control: max-age

Explanation:

Correct Answer: A

When a header "Cache-Control: no-cache, no-store" is set at the Origin server, Amazon CloudFront will retrieve content from the origin server when there is a request from the viewer. In some cases, if the origin server is not reachable, Amazon CloudFront will share a cached copy with the viewer.

To avoid such cases, the header can be set at the origin server as Cache-Control: stale-if-error=0. This will make sure that no cache copies are shared with the viewer. When there is a request from the viewer for private content and origin servers are not reachable, Amazon CloudFront will return an error.

Option B is incorrect as setting both headers max-age and s-maxage, Amazon CloudFront will cache the object for the duration lesser than s-maxage or default TTL specified.

Option C is incorrect as with setting expires header, Amazon CloudFront will cache the object until the date specified in the expire header.

Option D is incorrect as with removing the max-age header, Amazon CloudFront will cache the object for the duration of default TTL.

For more information on headers used for caching with Amazon CloudFront, refer to the following URL,

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Expiration.html#

Domain: Network Implementation

39. A financial institution has implemented hybrid connectivity using dual dedicated AWS Direct Connect links terminating at two different AWS locations. Link 1 has a bandwidth of 40 Gbps, while Link 2 has a bandwidth of 10 Gbps. The operations team is observing some of the asymmetric traffic flow, in which outbound traffic from AWS to on-premises location flows on Link 1 while incoming traffic to AWS cloud is on Link 2.

Operations Head has instructed you to make all traffic flow symmetric, making Link 1 as the primary link for communication between AWS cloud and on-premises location. Link 2 should be used as a secondary link for all communications.

How can BGP policy be set up at the customer end routers for making Link 1 as the primary link?

A> In Outbound BGP policy add AS_Path with 3 AS for prefixes advertised on Link 2. In inbound policy set the local preference as 80 for prefixes to be preferred on Link1.

B> In Outbound BGP policy add local preference as 300 for prefixes advertised on Link2. In inbound policy set the local preference as 80 for prefixes to be preferred on Link1.

C> In Outbound BGP policy add AS_Path with 1 for prefixes advertised on Link 2. In inbound policy set AS_Path as 2 for prefixes to be preferred on Link 1.

D> In Outbound BGP policy add AS_Path with 3 AS for prefixes advertised on link 2. In inbound policy set the local preference as 300 for prefixes to be preferred on Link1.

Explanation:

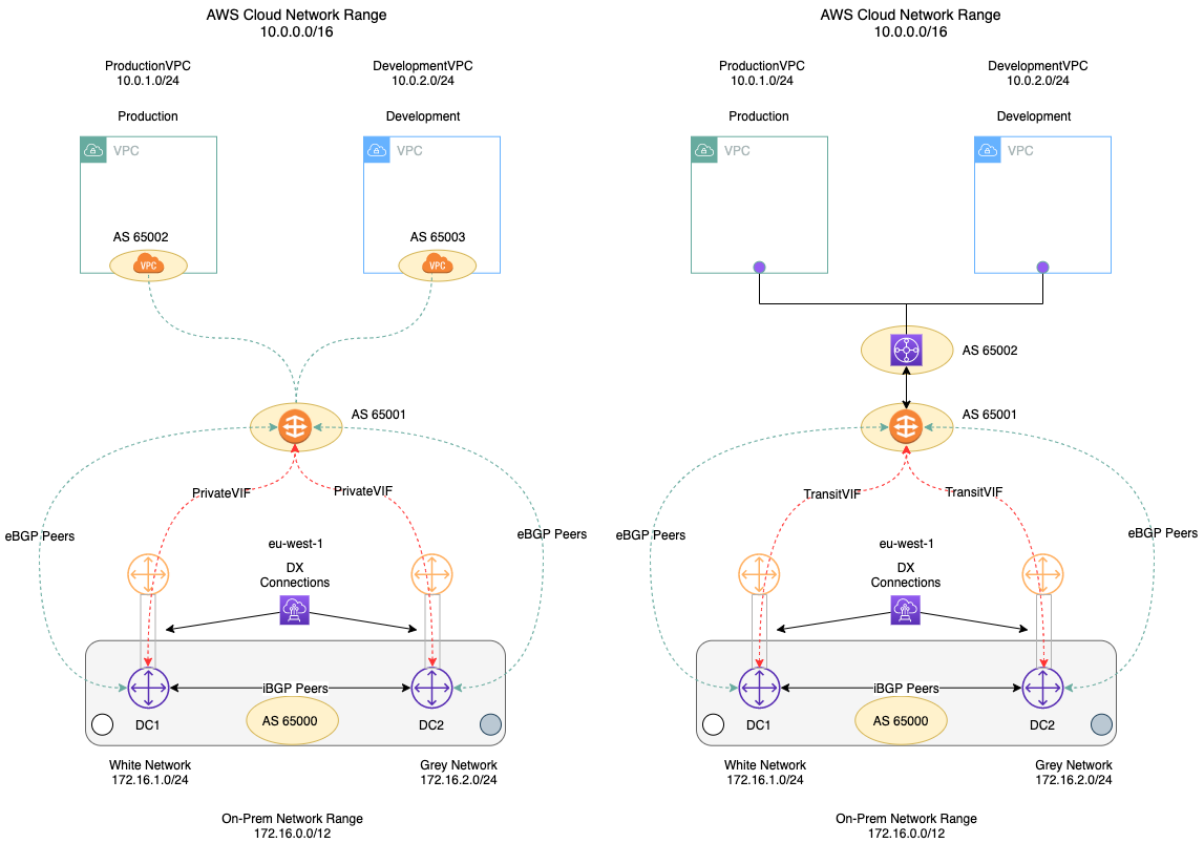
Correct Answer: D

BGP AS_Path attribute can be used to influence incoming traffic and is applied in outbound BGP policy. Shortest AS_Path is preferred. To prefer all incoming traffic on Link 1, AS_Path is set as 3 AS on Link 2. This will make Link 2 a less preferred path than Link 1 (which will have by default 1 AS) for traffic from the AWS cloud to the on-premises network. BGP Local Preference attribute is applied to the inbound route policy to influence all outgoing traffic. A Higher Local Preference value is preferred. Default Local preference value is 100.

To prefer outgoing traffic on Link 1, an inbound policy should be created to set the Local preference attribute as higher than the local preference value on Link 2. The local preference value of 300 can be set on Link 1 to prefer outgoing traffic.

Option A is incorrect as setting Local preference as 80 on Link 1 will make Link 2 (which will have default local preference as 100) the preferred path for outgoing traffic.**Option B is incorrect** as Outbound BGP Policy should alter AS_Path, not the Local Preference attribute. **Option C is incorrect** as the Inbound BGP policy should alter the Local Preference attribute, not the AS_Path attribute.

For more information on using BGP attributes for primary links, refer to the following URL,



https://aws.amazon.com/blogs/networking-and-content-delivery/creating-active-passive-bgp-connections-over-aws-direct-connect/

https://aws.amazon.com/blogs/aws/new-aws-direct-connect-gateway-inter-region-vpc-access/

https://aws.amazon.com/blogs/aws/new-use-an-aws-transit-gateway-to-simplify-your-network-architecture/

Domain: Network Design

40.You are working as an AWS consultant for a pharma company. For setting up a new TEST laboratory for R&D, the company plans to build a sub-1 Gig link to AWS. The new link should have a pre-defined SLA and consistent latency. Connectivity should be fully resilient and establish communication with all VPCs created within the organization in the region. Connectivity should be established in the shortest possible timeline.

What connectivity can be proposed to meet their requirement?

A> AWS Site-to-Site Managed VPN terminating on AWS Transit Gateway
B>AWS Direct Connect Hosted Connection terminating on AWS Transit Gateway
C> Dedicated AWS Direct Connect link terminating on Direct Connect Gateway

D> AWS Client VPN connecting to VPC via Client VPN endpoint

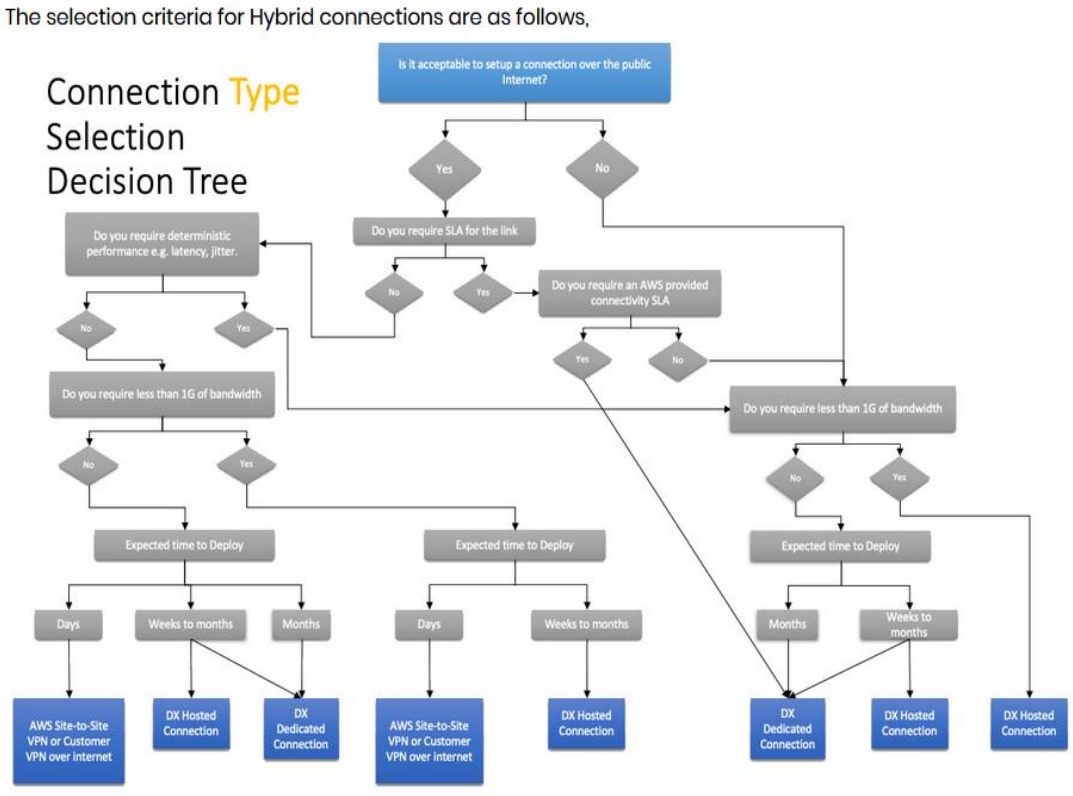
Explanation:

Correct Answer: B

There are two options for deploying sub 1Gbps links between on-premises location and AWS.

1. AWS Site-to-Site VPN: This is set up over the public internet. Latency on these links depends on the internet service provider network. This may vary as per congestion in the network. Also, no SLA is offered on this VPN connection.

2. AWS Direct Connect Hosted Connection: In hosted connection physical connectivity between the client & AWS is provided by the AWS Direct Connect partners. Since traffic is on private links, consistent latency is observed. AWS offers SLA on the Direct connect links for both dedicated as well hosted connections. With connection terminating on AWS Transit Gateway, connectivity to all VPCs in a region can be established.



Option A is incorrect as With Site-to-Site VPN terminating on AWS Transit Gateway, connectivity to all VPC in a region can be established. But AWS Site-to-Site Managed VPNs are created over the public internet and do not offer any SLA. **Option C is incorrect** as Dedicated AWS Direct connect links are available in 1 Gbps, 10 Gbps, and 100 Gbps. These are not available in sub-1

Gbps bandwidth. Deploying AWS direct connect hosted connection is faster than deploying a dedicated AWS Direct Connect link. The hosted connection can be deployed in a few weeks, while deploying dedicated direct connect links may take a longer time (approx. few months). **Option D is incorrect** as AWS Client VPN is created over the public internet and does not offer any SLA.

For more information on selecting the most suitable hybrid connectivity, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/connectivity-type-selection-summary.html

41. A global oil company has a head office located in London and regional offices in Paris and Sydney. They established hybrid connectivity using dedicated 10 Gbps AWS direct connect connections at all three locations.

A public virtual interface is created to access public AWS services at all these locations. Head-Office requires connectivity to public AWS services across the globe, while regional offices require connectivity to public AWS services for the region in which they are part of. The Head office should accept prefixes of public AWS services from the local continent while the regional office should accept public AWS services prefixes from the local region only. You have been assigned to implement BGP configuration on public virtual interfaces.

How can BGP community tags be attached at all three locations to meet these requirements?

A> For regional data centers, advertise prefixes with BGP community tag as 7224:8100 and accept prefixes with BGP community tag 7224:9100. For the head office, advertise prefixes with BGP community tag as 7224:8200 and accept all prefixes with community tags 7224:9200

B> For regional data centers, advertise prefixes with BGP community tag as 7224:9100 and accept prefixes with BGP community tag 7224:8100. For the head office, advertise prefixes with BGP community tag as 7224:9300 and accept all prefixes with BGP community tag as 7224:8200

C> For regional data centers, advertise prefixes with BGP community tag as 7224:9300 and accept prefixes with BGP community tag 7224:8200. For the head office, advertise prefixes with BGP community tag as 7224:9300 and accept all prefixes with community tags 7224:8100

D> For regional data centres, advertise prefixes with BGP community tag as 7224:8200 and accept prefixes with BGP community tag 7224:9200. For the head office, advertise prefixes with BGP community tag as 7224:8100 and accept all prefixes with community tags 7224:9100

Explanation:

Correct Answer: B

Customers can use BGP community tags to determine the scope of prefixes advertised to the AWS cloud. Following community tags can be used

i. 1.7224:9100-To advertise prefixes to Local AWS Region only.
ii. 2.7224:9200-To advertise prefixes to all AWS Regions for a continent.
iii. 3.7224:9300-To advertise prefixes to all public AWS Regions globally.

Since regional offices only need to advertise prefixes to local AWS regions, BGP community 7224:9100 should be tagged. At the head office, to advertise prefixes globally BGP community 7224:9300 should be tagged. AWS applies BGP community tags to prefixes advertised to customers. Following community tags are applied to determine which prefixes are advertised to the customer,

i. 1.7224:8100-To advertise prefixes from Local AWS Region only.
ii. 2.7224:8200-To advertise prefixes from all AWS Regions for a continent.
iii. No tag-To advertise prefixes from all public AWS Regions globally.

Since regional offices only need to have prefixes from the local AWS region, they can accept prefixes with BGP community 7224:8100. The BGP route policy can be configured at the head office to accept community 7224:8200.

Option A is incorrect as for advertising prefixes to AWS, customers should use either of the three communities, 7224:9100 or 7224:9200, or 7224:9300. While receiving prefixes from AWS, customers should match 7224:8100 or 7224:8200 or no tag. Option C is incorrect as regional data center advertising prefixes with tag 7224:9300 will advertise those prefixes globally which is not intended. Option D is incorrect as for advertising prefixes to AWS, customers should use either of the three communities, 7224:9100 or 7224:9200, or 7224:9300. While receiving prefixes from AWS, customers should match 7224:8100 or 7224:8200 or no tag.

For more information on BGP community tags for advertised and received prefixes over Public VIF, refer to the following URL,

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

Domain: Network Design

42. A global engineering company has two data centers in New York and Tokyo. The company has deployed application servers on Amazon EC2 instances in VPC created at four different AWS regions. You have been engaged in designing connectivity

between these data centers and VPC. All VPCs should be able to communicate with all other VPCs as well as with both the data centers. The proposed connectivity should integrate data centers with any new AWS region in which the application will be deployed in the future.

Which design can be proposed to provide full resiliency?

A> Set up dual Direct Connect links terminating on two different Direct Connect Gateway from each Data Centre. Connect one Direct Connect gateway to three AWS Transit Gateways attached in three separate regions while another Direct Connect gateway to one Transit gateway attached to one region. Configure full mesh peering between four Transit Gateways created in each of the four regions.

B> Set up dual Direct Connect links terminating on a single Direct Connect Gateway from each Data Centre. Connect one Direct Connect gateway to four AWS Transit Gateways attached to four separate regions. Configure full mesh peering between four Transit Gateways created in each of the four regions.

C> Set up dual Direct Connect links terminating on a single Direct Connect Gateway from each Data Centre. Connect one Direct Connect gateway to four Virtual Private gateways attached to four separate regions. Configure full mesh VPC peering between VPCs in different regions.

D> Set up dual Direct Connect links terminating on two different Direct Connect Gateway from each Data Centre. Connect one Direct Connect gateway to two Virtual Private gateways attached to two separate regions while another Direct Connect gateway to two Virtual Private gateways attached to two separate regions. Configure full mesh VPC peering between VPCs in different regions.

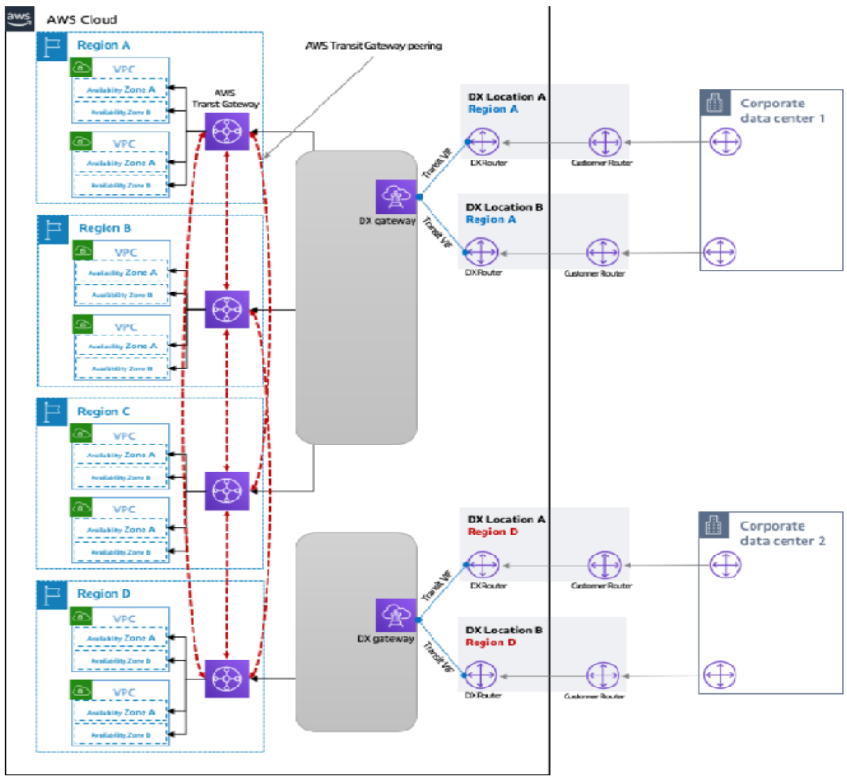
Explanation:

Correct Answer: A

Connectivity can be designed as follows,

1. Two data centers can have dual AWS Direct Connect links terminating at two different Direct Connect Gateway. This will provide resiliency at the link level as well as location level. A single Transit virtual interface can be created on each of these links.
2. VPCs in each of the four regions can connect with a single AWS Transit gateway attached to each region. Cross-region VPC communication can be provided by peering through the AWS Transit gateway attached to each region. The same infrastructure setup can be used for any new VPC created in these four regions.
3. Each AWS Direct Connect Gateway can connect a maximum of up to three AWS Transit Gateways. To have connectivity with VPC in four different regions, one Direct Connect Gateway can have connectivity with three Transit Gateways while other Direct Connect Gateways can have connectivity with one Transit Gateway. This will provide communication between data centers at both locations New York and Tokyo with VPCs in all four regions.

4. For all future applications to be deployed in new regions, if the count of regions is more than 3 per Direct Connect Gateway, an additional Direct Connect Gateway can be set up.
5. Route-summarization can be configured to avoid maximum prefix count limits.
    i. Number of prefixes from on-premises to AWS on a transit virtual interface: 100
    ii. Number of prefixes per AWS Transit Gateway from AWS to on-premises on a transit virtual interface: 20



Option B is incorrect as only three AWS Transit gateways can be connected per Direct Connect Gateway. **Option C is incorrect** as full Mesh VPC peering will add complexity & additional management overhead to configure peering for any new VPC created in any of the regions. Also, connecting both data centers to a single Direct Connect Gateway will lead to a single point of failure. **Option D is incorrect** as full Mesh VPC peering will add complexity & additional management overhead to configure peering for any new VPC created in any of the regions.

For more information on connecting VPC & on-premises locations in multi-region, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-aws-transit-gateway-multi-regions-more-than-3.html

Domain: Network Design

43. An IT firm has created 3 VPCs with subnet as 10.10.1.0/24 for VPC A, 10.10.2.0/24 for VPC B, and 10.10.3.0/24 for VPC C. All these three VPCs need to communicate only with a VPN connection which has subnet as 10.10.10.0/24. There should not be any communication between these 3 VPCs. Routing at VPC & VPN customer gateway routers is taken care of by the IT team internally. They seek your guidance as an AWS expert to design AWS Transit Gateway Route tables.

How can Transit Gateway Routing be done to meet this requirement?

A. Create two tables with AWS Transit Gateway (Refer Table-1). Associate VPC Attachments with a route table that has routes propagated from VPN (Refer Table-2)

Table 1 AWS transit Gateway

Destination	Target	Route type
10.10.10.0/24	Attachment for VPN connection	propagated

Table 2 VPC Attachment Route Table

Destination	Target	Route type
10.10.1.0/24	Attachment for VPC A	propagated
10.10.2.0/24	Attachment for VPC B	propagated
10.10.3.0/24	Attachment for VPC C	propagated

B. Create a single route table with AWS Transit Gateway.

Destination	Target	Route type
10.10.1.0/24	Attachment for VPC A	propagated
10.10.2.0/24	Attachment for VPC B	propagated
10.10.3.0/24	Attachment for VPC C	propagated

C. Create two tables with AWS Transit Gateway (Table-1). Associate VPC Attachments with a route table that has routes propagated from VPN.

Table 1 AWS transit Gateway

Destination	Target	Route type
0.0.0.0/0	Attachment for VPN connection	static

Table 2 VPC Attachment Route Table

Destination	Target	Route type

10.10.1.0/24	Attachment for VPC A	propagated
10.10.2.0/24	Attachment for VPC B	propagated
10.10.3.0/24	Attachment for VPC C	propagated

D. Create single route table with AWS Transit Gateway

Destination	Target	Route type
10.10.1.0/24	Attachment for VPC A	propagated
10.10.2.0/24	Attachment for VPC B	propagated
10.10.3.0/24	Attachment for VPC C	propagated
0.0.0.0/0	Attachment for VPN connection	static

Explanation:

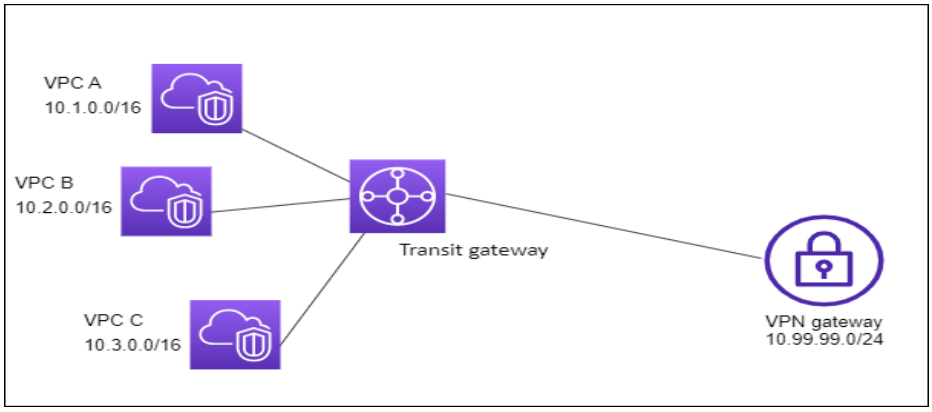
Correct Answer: A

AWS Transit Gateway can be configured as multiple isolated routers. With this setup, attachments associated with an isolated router can communicate with each other but cannot communicate with attachments associated with another isolated router. In the above case, VPC A, VPC B, and VPC C need to communicate with the VPN subnet, but there should be communication between these VPCs. Two separate route tables need to be created in AWS Transit Gateway. One route table will have routes propagated from VPN connections associated with VPC attachments. Another route table will have routes propagated from all three VPC attachments & will be associated with VPN attachments.

Option B is incorrect as this will allow communication between all three VPC to VPN connections. But it will also allow communication among all three VPCs which is not expected. **Option C is incorrect** because all traffic not matching in the routing table will be routed to a VPN connection due to the default static route. This is not as per expectation. VPC A, VPC B, and VPC C should only communicate with VPC subnet 10.10.10.0/24.**Option D is incorrect** as this will allow communication between all three VPC to VPN connections. But it will also allow communication among all three VPCs which is not expected. Also, all traffic not matching in the routing table will be routed to a VPN connection due to the default static route.

The following diagram shows the key components of the configuration for this scenario. Packets from VPC A, VPC B, and VPC C route to the transit gateway. Packets from the subnets in VPC A, VPC B, and VPC C that have the internet as a destination first route through the transit gateway and then route to the Site-to-Site VPN connection (if the destination is within that network). Packets from one VPC that have a destination of a subnet in another VPC, for

example from 10.1.0.0 to 10.2.0.0, route through the transit gateway, where they are blocked because there is no route for them in the transit gateway route table.



For more information on the isolated routers with AWS Transit Gateway, refer to the following URL,

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-isolated.html

Domain: Network Design

44. A pharma company is building hybrid connectivity between an on-premises location and the AWS cloud. This connectivity will be used by a critical application to access data from Amazon EC2 instances in multiple VPCs. The project team has configured a dual Site-to-Site VPN terminating on an AWS Transit Gateway with VPN dead peer detection for resiliency. After the deployment, the application team raises concerns about the application performance on Site-to-Site VPN links. On-premises location is using IPCIDR block of 10.20.30.0/24. As a consultant, you are required to provide suggestions for maximizing performance efficiency on dual Site-to-Site VPN links along with resiliency.

Which of the following additional configurations will provide the performance efficiency required for this application?

A> Configure ECMP on each VPN connection terminating on AWS Transit Gateway. Advertise different specific routes (10.20.30.0/25 & 10.20.30.128/25) on each VPN link over BGP peering.

B> **Configure ECMP on each VPN connection terminating on AWS Transit Gateway. Advertise different specific routes (10.20.30.0/25 & 10.20.30.128/25) on each VPN link along with summarised routes (10.20.30.0/24) over BGP peering.**

C> Configure ECMP on each VPN connection terminating on AWS Transit Gateway. Advertise default routes (0.0.0.0/0) on one VPN link while summarised routes (10.20.30.0/24) over another VPN link.

D> Configure ECMP on each VPN connection terminating on AWS Transit Gateway. Advertise default routes (0.0.0.0/0) on one VPN link while a specific route (10.20.30.0/25) over another VPN link.

Explanation:

Correct Answer: B

Configuring ECMP on VPN links will increase overall VPN link bandwidth by using both links for traffic between AWS & on- premises locations. When specific routes (10.20.30.0/25 & 10.20.30.128/25) are advertised on each link along with summarised routes (10.20.30.0/24), during a normal scenario when both links are UP, traffic for 10.20.30.0/25 will prefer VPN link 1 while traffic for 10.20.30.128/25 will prefer VPN link 2. When any one of the links is down, traffic will prefer another link as it has a summarised route advertised.

Option A is incorrect as this would distribute traffic across both VPN links. But if any one of the links is down, it would impact traffic to the subnet advertised from that VPN link. If the VPN link which advertises 10.20.30.0/25 is down, traffic to this subnet from AWS will be impacted as this subnet is not advertised from another VPN link.

Option C is incorrect. As with this configuration, traffic will be flowing only on the VPN link with the summarised route (10.20.30.0/24) as route selection will be based on the IP prefix longest match.

Option D is incorrect as this will provide redundancy for the specific route. But it would not provide any redundancy when the VPN link which advertises the default route is down.

For more information on Dual Site-to-Site VPN connections with more specific routes, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/dual-site-to-site-vpn-connections-with-more-specific-routes-example.html

Domain: Network Security, Compliance, and Governance

45. A company uses hybrid connectivity from an on-premises location to AWS using AWS Direct Connect & terminates on AWS Transit Gateway. Nodes at on-premises access application deployed on Amazon EC2 instance in multiple VPCs. Amazon EC2 network instance workload shares the same subnet with that of AWS Transit gateway association. During the Security audit, it was found that Network ACLs are missing & needs to apply immediately to meet security compliance. You have been assigned to configure Network ACL on these subnets.

How can network ACLs be configured for traffic flowing from the Amazon EC2 instance to the Transit gateway?

A> Create inbound rules which use a source IP address for evaluation while Outbound Rules are not required to be evaluated.
B> Create outbound rules which use a source IP address for evaluation while inbound rules are not required to be evaluated.
C> Create outbound rules which use a destination IP address for evaluation while inbound rules use a source IP address for evaluation.
D> Create inbound rules which use a destination IP address for evaluation while outbound rules use a source IP address for evaluation.

Explanation:

Correct Answer: C

While creating Network ACL for traffic flowing from Amazon EC2 instance to AWS Transit Gateway, they both (EC2 network interface workload & Transit gateway) are part of the same subnet; the following rules are applied,

1. *Outbound rules use the destination IP address for evaluation.*
2. *Inbound rules use the source IP address for evaluation.*

For traffic from transit gateway to Amazon EC2 instance, Outbound & inbound rules are not required to be evaluated.

Option A is incorrect. As traffic flows from the Amazon EC2 instance to Transit Gateway, outbound rules need to be evaluated based on the destination IP address.

Option B is incorrect. As traffic flows from the Amazon EC2 instance to Transit Gateway, inbound rules need to be evaluated based on the source IP address.

Option D is incorrect. As inbound rules use the source IP address, Outbound rules use the destination IP address for evaluation.

For more information on NACL with AWS Transit Gateway, refer to the following URL,

https://docs.aws.amazon.com/vpc/latest/tgw/tgw-nacls.html

Domain: Network Implementation

46. An IT firm has created VPC A & VPC B which are associated with AWS Transit Gateway. Recently they have deployed a new shared services VPC C with a third-party security appliance and associated with a transit gateway. All traffic from VPC A & VPC B must be routed to a security appliance in VPC C for security inspection before it is forwarded to the destination. VPC C has two subnets, one for the Transit gateway and the other for appliances. Routing for AWS Transit Gateway is done & IT team is looking for your suggestions for creating routing entries in VPC A, VPC B, and VPC C.

How do route tables in VPC A, VPC B, and VPC C need to be set up to meet this requirement?

A> Create a route table in both VPC A & VPC B having a default route pointing to the Transit gateway. For VPC C, in the transit gateway subnet, create a specific route of VPC A and VPC B subnets with targets as VPC A & VPC B respectively. For VPC C, in the appliance subnet, create a default route pointing to the Transit gateway. For VPC attachments in shared services VPC, enable appliance mode.

B> Create a route table in both VPC A & VPC B having a default route pointing to the Transit gateway. For VPC C, in the transit gateway subnet, create a default route with the target as appliance in the appliance subnet. For VPC C, in the appliance subnet, create a default route pointing to VPC A and VPC B. For VPC attachments in VPC A & VPC B, enable appliance mode.

C> Create a route table in both VPC A & VPC B having a default route pointing to the appliance subnet in VPC C. For VPC C, in transit gateway subnet, create a default route with the target as an appliance in appliance subnet. For VPC C, in the appliance subnet, create a default route pointing to the Transit gateway. For VPC attachments in VPC A & VPC B, enable appliance mode.

D> **Create a route table in both VPC A & VPC B having a default route pointing to the Transit gateway. For VPC C, in the transit gateway subnet, create a default route with the target as an appliance in the appliance subnet. For VPC C, in the appliance subnet, create a default route pointing to the Transit gateway. For VPC attachments in shared services VPC, enable appliance mode.**

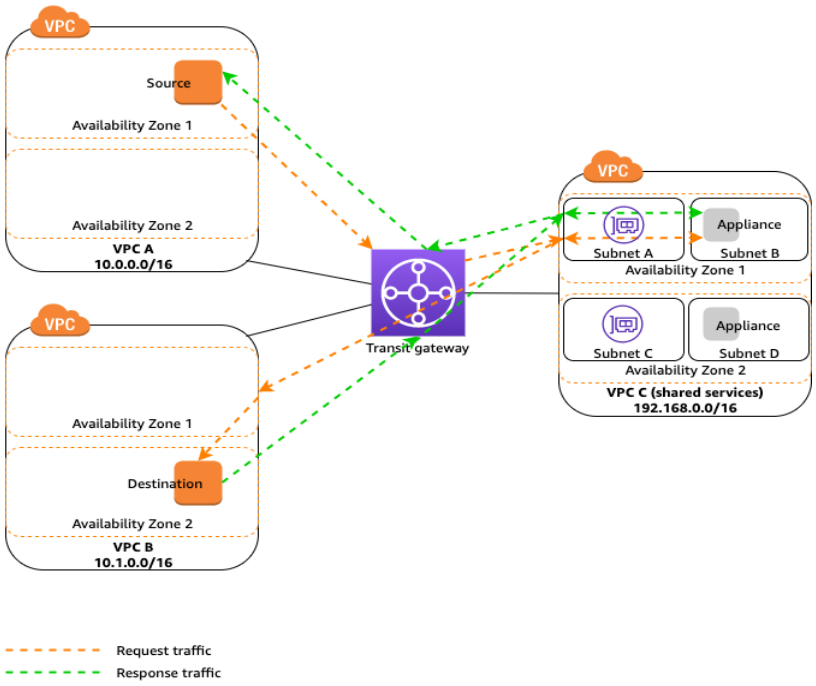
Explanation:

Correct Answer: D

With appliance mode enabled for VPC attachments in VPC C, the transit gateway will select a single network interface for both forward & return traffic, ensuring bidirectional symmetric traffic. Routing for VPC A, VPC B & VPC C should be as follows,

1) In VPC A & VPC B, all traffic should be passing through the transit gateway. For this, a default route entry should be added to the routing table with the target as the transit gateway.
2) In VPC C, there should be 2 different route tables for each subnet: transit gateway subnet and appliance subnet. In the Transit Gateway subnet route table, all traffic should have a target to the appliance in the appliance subnet. For return traffic from the appliance to VPC A and VPC B, the appliance subnet should have a default route entry with the target as the transit gateway.

   Traffic flow is as depicted in the following diagram,



Option A is incorrect as in the transit gateway subnet of VPC C the default route should be added with the target as an appliance in the appliance subnet, not the specific route of VPC A & VPC B subnets.

Option B is incorrect as in the appliance subnet of VPC C, default routes should have a target as transit Gateway & not directly to VPC A and VPC B. Appliance mode should be enabled on transit gateway attachments in VPC C & not in VPC A and VPC B.

Option C is incorrect as in VPC A & VPC B all default routes should be targeted to AWS Transit gateway & not to appliance subnet in VPC C. Appliance mode should be enabled on transit gateway attachments in VPC C & not in VPC A and VPC B.

For more information on using appliance mode with share services VPC, refer to the following URL,

https://docs.aws.amazon.com/vpc/latest/tgw/transit-gateway-appliance-scenario.html

Domain: Network Design

47. A State University has deployed e-learning educational courses on Amazon EC2 instances in a service consumer VPC. These courses are accessed by global users via the Internet Gateway attached to this VPC. To strengthen the security of these media, they have deployed a security appliance & Gateway Load Balancer in the service provider VPC. The Gateway Load Balancer endpoint is created in the service consumer VPC. The Amazon EC2 instance is part of the application server subnet while the Gateway endpoint is part of the Gateway Load Balancer endpoint subnet. All traffic flow to and from the Internet via the Internet Gateway from the service consumer VPC should be flowing via the security appliance in the security provider

VPC where the traffic will be intercepted to identify any malware or security breaches.

The IT Team from this university is looking for your suggestions for configuring routing tables at the Internet gateway, Service consumer VPC & in the Gateway Load Balancer endpoint subnet.

Which of the following are the correct route table entries that need to be configured?

A>

i. In the Internet Gateway route table, for the destination as application server's subnet target should be the Gateway Load Balancer endpoint.
ii. In the Application server subnet, the default route should be added with Target as Internet Gateway.
iii. In the Gateway Load Balancer endpoint subnet, the default route should be added with Target as the Internet gateway.

B>

i. In the Internet Gateway route table, for the destination as application server's subnet target should be the Gateway Load Balancer endpoint.
ii. In the Application server subnet, the default route should be added with Target as the Gateway Load Balancer endpoint.
iii. In the Gateway Load Balancer endpoint subnet, the default route should be added with Target as the Internet gateway.

C>

i. In the Internet Gateway route table, for the destination as application server's subnet target should be the Security appliance subnet.
ii. In the Application server subnet, the default route should be added with Target as the Gateway Load Balancer endpoint.
iii. In the Gateway Load Balancer endpoint subnet, the default route should be added with Target as Security appliance subnet.

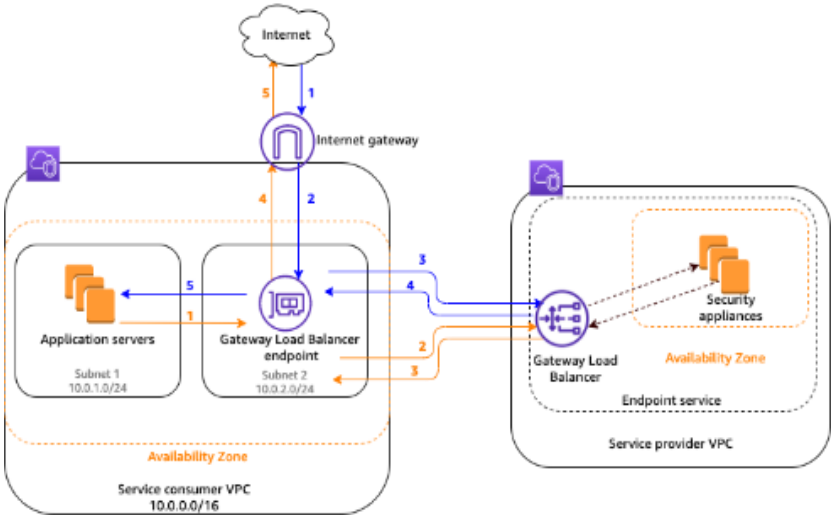
D>

i. In the Internet Gateway route table, for the destination as application server's subnet target should be Security appliance subnet.
ii. In the Application server subnet, the default route should be with Target as Internet Gateway.
iii. In the Gateway Load Balancer endpoint subnet, the default route with Target as Internet Gateway

Explanation:

Correct Answer: B

Traffic flow from Amazon EC2 instance to and from Internet Gateway Load Balancer endpoint is as shown in below diagram



Routing entries should be added based on the following logic,

1) For all traffic from the Internet towards the Amazon EC2 instance in the application server subnet, it should hit the Gateway Load Balancer endpoint.
2) In the application server subnet, all traffic destined to the Internet should first hit the Gateway Load Balancer endpoint.
3) For all traffic receiving from security appliances to Gateway Load Balancer endpoint which has destination as application server subnet, they already have a local route in the routing table since both Gateway Load Balancer endpoint & application server are part of the same VPC.
4) For all traffic receiving from the security appliance to Gateway Load Balancer endpoint which has destination as Internet, a default route needs to be added pointing to Internet Gateway.

Option A is incorrect as a default route for application server subnet should have the target as Gateway Load Balancer endpoint & not Internet gateway since all traffic should pass via security appliance in service provider VPC.

Option C is incorrect as in the Internet Gateway route table, for the destination as application server subnet, the target should be gateway load balancer endpoint and not security appliance subnet. Also, in the Gateway Load Balancer endpoint subnet, the default route should be added with Target as Internet Gateway and not the Security appliance subnet.

Option D is incorrect as in the Internet Gateway route table, for the destination as application server subnet, the target should be gateway load balancer endpoint & not security appliance subnet. Also, in the application

server subnets should have a target as a Gateway Load Balancer endpoint & not an Internet gateway.

For more information on using appliance mode with share services VPC, refer to the following URL,

https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/getting-started.html

Domain: Network Design

48. A company has deployed a new application in AWS Cloud. The peak requirement for this application would be 2 Gbps. The company plans to use AWS Direct Connect for this requirement To access this application from an on-premises location. Connectivity should be fully resilient with proper backup solutions in place For this critical application. Any outage in the links will lead to a huge financial impact on the company.

Which of the following solutions can be implemented to provide maximum resiliency for critical applications without any performance degradation?

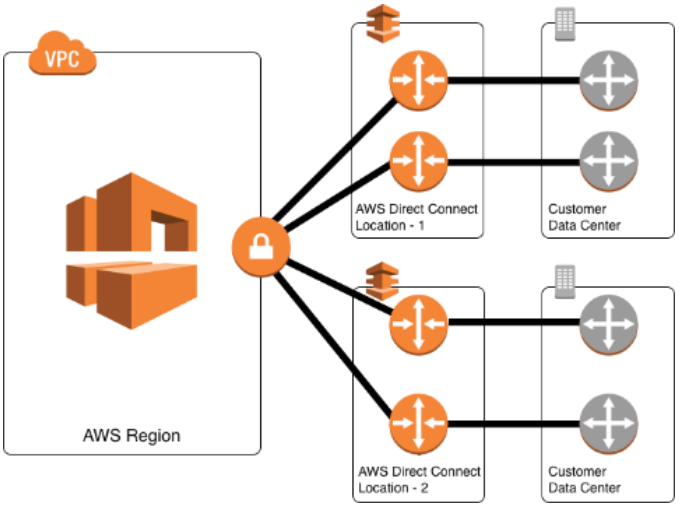
A> Create a new 2 GB AWS Direct link backing with a VPN connection of 2 Gb.
B> Create two new 2 GB AWS Direct links at a single AWS Direct Connect location with links terminating on two different routers.
C> Create a new 2 GB AWS Direct link with links terminating at two AWS Direct Connect locations on two different routers.
D> Create a new 2 GB AWS Direct link with links terminating at two AWS Direct Connect locations on a single router.

Explanation:

Correct Answer: C

Links need to be terminated on two separate routers at each Direct Connect location to get maximum resiliency on AWS Direct Connect links. AWS Direct Connect links also need to be terminated at two different AWS Direct Connect locations to get location-level redundancy. This type of connectivity will provide router level as well as location level resiliency for the critical application.

The following diagram shows AWS Direct Connect connectivity with maximum resiliency,



Option A is incorrect as the application may face performance issues on the VPN link when the AWS Direct Connect link is down.

Option B is incorrect as it may result in an outage since the company is looking for maximum resiliency if there are issues at one AWS Direct connect location.

Option D is incorrect as this will not provide router-level redundancy at each AWS Direct connect location.

For more information on redundancy with AWS Direct Connect, refer to the following URL,

https://aws.amazon.com/directconnect/resiliency-recommendation/

Domain: Network Security, Compliance, and Governance

49. A healthcare company is setting hybrid connectivity using AWS Direct Connect between on-premises locations and the AWS cloud. They are looking for securing all types of data including control plane traffic flowing over this link. The proposed solution should not impact data speed for the traffic.

Which of the following encryption solutions is best suited to meet this requirement?

A> Use SSL/TLS encryption for applications over AWS Direct Connect.
B> Use IPsec VPN over AWS Direct Connect.
C> Use MACsec with AWS Direct Connect.
D> Use GRE VPN over AWS Direct Connect.

Explanation:

Correct Answer: C

MACsec is a Layer 2 encryption service that provides Layer 2 confidentiality and integrity to all control plane protocols. With MACsec, encryption is done using hardware that provides high-speed encryption. MACsec can be used for 10 Gbps and 100 Gbps AWS Direct Connect links providing high-speed data encryption from an on-premises location to AWS.

Option A is incorrect as SSL/TLS encryption will work qt upper layers & will not provide high-speed encryption for ethernet connections, including control plane protocols.

Option B is incorrect as IPsec VPN over AWS Direct Connect will work at upper layers and will not provide high- speed encryption for ethernet connections, including control plane protocols.

Option D is incorrect as GRE tunnels will provide encapsulation & not encryption of data over AWS DirectConnect.

For more information on LAGS with AWS Direct Connect, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/adding-macsec-security-to-aws-direct-connect-connections/

Domain: Network Design

50. An insurance company is planning to set up hybrid connectivity between on-premises locations & AWS. To establish this connectivity, the company has procured a 500 Mbps hosted connection from the AWS Direct Connect partner. Multiple VPCs created in different regions need to be accessed from a single on-premises location.

What solution can be designed to implement this connectivity in the simplest way?

A> Create a transit virtual interface to Direct Connect Gateway & terminate it to AWS Transit gateway which has VPC attachments to multiple VPCs in different regions.

B> Create a public virtual interface to the Direct Connect gateway & terminate it to the AWS Transit gateway which has VPC attachments to multiple VPCs in different regions.

C> Create a public virtual interface over this connection. Establish VPN over this AWS Direct Connect & terminate it to AWS Transit gateway which has VPC attachments to multiple VPCs.

D> Create a transit virtual interface over the Direct Connect link. Establish VPN over this AWS Direct Connect and terminate it to AWS Transit gateway which has VPC attachments to multiple VPCs.

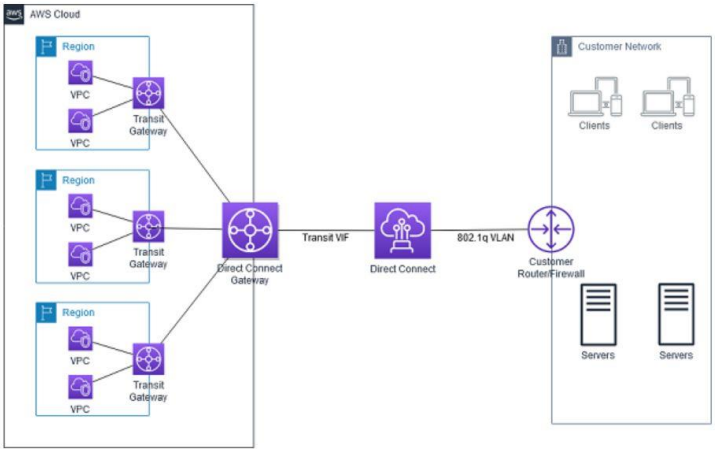
Explanation:

Correct Answer - A

AWS Transit Gateway can be used as a transit hub to connect multiple VPCs from on-premises locations. For this, a transit virtual interface is created with AWS Direct Connect and is used with AWS Transit Gateway. Using this connectivity, a single Direct Connect Link can help to connect to multiple VPCs resulting in a simpler cost-effective solution. AWS Direct Connect supports any speed links to AWS Transit Gateway. For connecting to VPC in

different regions, the Direct Connect gateway can be used to connect to Transit gateways in multiple regions. Transit Virtual interface can be used for dedicated as well for hosted connections of any speed. And TGW now supports sub 1 Gbps connections.

The following diagram shows connectivity from an on-premise location to multiple VPCs using AWS Transit Gateway and Direct Connect.



Option B is incorrect as for connecting AWS Direct Connect on AWS Transit Gateway, a transit virtual interface is required and not a public virtual interface. **Option C is incorrect** as although this will work, this will require additional configurations to create a VPN over AWS Direct connect. Using the Transit Virtual Interface to AWS Transit Gateway will be a simpler solution to deploy. **Option D is incorrect** as a VPN connection over AWS Direct Connect should be created on the public virtual interface and not on a transit virtual interface.

For more information on connecting multiple VPCs using AWS Transit Gateway, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-direct-connect-aws-transit-gateway.html

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

Domain: Network Management and Operation

51. A company has deployed an AWS CloudFront distribution with AWS Application Load Balancer as the origin. AWS Application Load Balancer further distributes

traffic to Amazon EC2 instances deployed in multiple availability zones. The operations team monitoring this traffic observes that some of the user sessions are directly terminating on the Application Load balancer instead of via AWS CloudFront. This leads to additional load on Application Load Balancer. *Which of the following actions can be initiated to overcome this problem?*

A> Configure host firewall on Amazon EC2 instance & allow only CloudFront CIDR ranges to access.

B> Add custom headers in Amazon CloudFront & configure ALB to forward requests containing only custom headers to the EC2 Instance.

C> Create a security group for Application Load Balancer which will allow only Amazon CloudFront CIDR ranges.

D> Use WAF at both AWS CloudFront & AWS Application Load Balancer to restrict direct access to the internet.

Explanation:

Correct Answer: B

Following steps can be initiated to restrict users from directly accessing Application Load Balancer instead of from Amazon CloudFront,

1) Configure Amazon CloudFront to add custom HTTP headers to all requests which are forwarded to the Application Load balancer.
2) Configure Application Load Balancer to forward only those requests which have custom headers to Amazon EC2 instances.

This will ensure that no users can directly access the Application Load balancer & increase its load. Also, when all users are accessing applications via Amazon CloudFront, it will help to decrease latency as well as protect from Distributed denial of service (DDOS) attacks.

Option A is incorrect as configuring a host-based firewall will be additional admin work. Also, since the Application load balancer is front-ending these instances, the instance will be receiving traffic from the Application Load balancer IP address. **Option C is incorrect** as this will add complexity to managing & updating security groups with a large number of Amazon CloudFront CIDR ranges. **Option D is incorrect** as although this will work, this will lead to additional latency to traffic because of dual WAF rules checking.

For more information on restricting access to the Application load balancer front-ended by Amazon CloudFront, refer to the following URL,

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/restrict-access-to-load-balancer.html

Domain: Network Design

52. A streaming provider uses Amazon CloudFront to distribute content to users across the globe. The marketing team is looking for users' physical locations to get the popularity of the content region-wise. The application team has suggested performing HTTP header manipulation by adding HTTP header True-Client-IP to the viewer request. As an AWS expert, you have been assigned to create a function for this requirement & deploy it at the Amazon CloudFront.

Which functions can be configured at CloudFront to get these details?

A> Use Lambda@Edge function & execute at the edge location.
B> Use CloudFront functions & execute at the regional edge location.
C> Use Lambda@Edge & execute at the regional edge location.
D> Use CloudFront functions & execute at the edge location.

Explanation:

Correct Answer: D

CloudFront functions are suitable for performing lightweight short-running functions from edge locations. CloudFront Functions are suitable for running the following functions,

- Cache key normalization
- Header manipulation
- URL redirects or rewrites

Request authorization

In the above case, the customer needs to perform Header manipulation by adding the True-Client-IP header to the viewer request. This can be done using the CloudFront function & can be executed from the edge location.

Option A is incorrect as for HTTP header manipulation, CloudFront functions are a better option than Lambda@Edge. Also, Lambda@Edge cannot be executed from edge locations. Lambda@Edge functions are executed from regional cache locations. **Option B is incorrect** as CloudFront functions run from edge locations & not from regional edge locations. **Option C is incorrect** as for HTTP header manipulation, CloudFront functions are a better option than Lambda@Edge as these are less expensive.

For more information on CloudFront functions, refer to the following URL,

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/edge-functions.html

Question 33 of 65

Domain: Network Implementation

53. An IT firm plans to deploy a new application that works on IPv6 addresses. A VPC with IPv4 address is already created with an Amazon EC2 instance deployed. For securing Amazon EC2 instances, security group & custom network ACL are configured. As a Network design lead, you have been asked to work on existing VPC to support IPv6.

What steps can be performed to have an existing VPC with IPv4 addressing migrated to IPv6 addressing?

A>Associate an IPv6 CIDR block to VPC & subnets. Update Route tables & security group rules to include IPv6 addresses. Manually add IPv6 subnets in custom network ACL created for IPv4 subnets. Select instance type supporting IPv6 & assign IPv6 to the instance.

B> Associate an IPv6 CIDR block to subnets. Update Route tables & security group rules automatically updated with IPv6 addresses. IPv6 subnets are automatically added to custom network ACL created for IPv4 subnets. Select instance type supporting IPv6 & assign IPv6 to the instance.

C> Disable IPV4 support to VPC & associate an IPv6 CIDR block to VPC & subnets. Update Route tables & security group rules to include IPv6 addresses. Manually add IPv6 subnets in custom network ACL created for IPv4 subnets. Select instance type supporting IPv6 & assign IPv6 to the instance.

D> Disable IPV4 support to VPC & associate an IPv6 CIDR block to subnets rules automatically updated with IPv6 addresses. Update Route tables & security group rules to include IPv6 addresses. IPv6 subnets are automatically added to custom network ACL created for IPv4 subnets. Select instance type supporting IPv6 & assign IPv6 to the instance.

Explanation:

Correct Answer: A

For Associating IPv6 CIDR to existing VPC, the following steps are required,

1) Associate an IPv6 CIDR block with VPC and subnets- New IPv6 CIDR block needs to be associated with both VPC &subnets.
2) Update route tables-Update route tables with IPv6 subnets.
3) Update security group rules & network ACL - need to manually update security groups with new IPv6 subnets. If the existing VPC has default Network ACL, IPv6 subnets are automatically updated. In the case of custom network ACL, rules need to be manually updated in network ACL for IPv6 subnets.
4) Change instance type-Only required if the existing EC2 instance is an old generation instance.
5) Assign IPv6 addresses to your instances.
6) Configure IPv6 on your instances- This is an optional step required depending upon AMI used for Amazon EC2 instances.

Option B is incorrect as Security Group rules are not automatically updated with IPv6 subnets. It needs to be manually updated. Custom network

ACL created for IPv4 subnets needs to be manually updated with IPv6 subnets & are not automatically updated.
Option C is incorrect as for associating IPv6 CIDR block to VPC, IPv4 is not required to be disabled.
Option D is incorrect as for associating IPv6 CIDR block to VPC, IPv4 is not required to be disabled. Custom network ACL created for IPv4 subnets needs to be manually updated with IPv6 subnets.
For more information on associating IPv6 with VPC, refer to the following URL,
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-migrate-ipv6.html

Domain: Network Implementation

54. An R&D firm has built a new graphics-intensive application that requires a very low latency for better performance. Users will be accessing this application from an on-premises location. The firm has already deployed services in the AWS cloud. All services deployed in the data center will gradually be moved to AWS Cloud. This application will be using Amazon S3 for storage which should be accessible with optimum latency.

Which solution can be implemented to meet this requirement?

A> Extend subnets from parent AWS VPC to AWS Outpost. Deploy the application in the AWS Outpost. Access Amazon S3 privately using the Gateway endpoint.
B> Extend subnets from parent AWS VPC to AWS Local Zone. Deploy the application in the AWS Local Zone. Access Amazon S3 privately over AWS Private network.
C> Extend subnets from parent AWS VPC to AWS Local Zone. Deploy the application in the AWS Local Zone. Access Amazon S3 privately using the Gateway endpoint.
D> Extend subnets from parent AWS VPC to AWS Outpost. Deploy the application in the AWS Outpost. Access Amazon S3 privately over AWS Private network.

Explanation:
Correct Answer: B

AWS Local Zones can be used to deploy certain AWS services like compute & storage services (Amazon EC2, Amazon EBS, Amazon FSX, etc.) closer to end-users. This will help to access AWS services with less latency. VPC from the parent region is extended to AWS Local Zones. Other AWS services like Amazon S3 hosted in parent regions are accessible via VPC over AWS private network which helps in low latency for applications hosted in AWS Local Zones.

Option A is incorrect as AWS Outpost needs to be deployed in a local data center. Since the customer is moving all services out of the data center, this is not a better option. **Option C is incorrect** as Amazon S3 is privately accessible over AWS Private network from AWS Local zone. There is no need to access via the S3 Gateway endpoint. **Option D is incorrect** as AWS Outpost needs to be deployed in a local data center. Since the customer is moving all services out of the data center, using AWS Local Zones is a better option.
For more information on AWS Local Zones, refer to the following URL,
https://aws.amazon.com/about-aws/global-infrastructure/localzones/faqs/

Question 35 of 65 Domain: Network Security, Compliance, and Governance

55. An IT firm has deployed Kubernetes clusters using Amazon Elastic Kubernetes Service (Amazon EKS). These clusters are deployed in multiple member accounts which are part of AWS Organisation. They are using Amazon GuardDuty for monitoring security in all accounts. The Security Team is looking for the suspicious activity being carried out in Amazon EKS.

What steps can be taken to check GuardDuty findings from this Elastic Kubernetes Service (Amazon EKS)?

A> Enable Kubernetes protection for all member accounts in an Organisation using GuardDuty member accounts. Retrieve GuardDuty findings through logs stored in Amazon S3 buckets.
B> Enable Kubernetes protection for all member accounts in an Organisation using GuardDuty delegated administrators accounts. Retrieve GuardDuty findings through logs stored in Amazon S3 buckets.
C> Enable Kubernetes protection for all member accounts in an Organisation using GuardDuty delegated administrators accounts. Retrieve GuardDuty findings through Amazon CloudWatch events.
D> Enable Kubernetes protection for all member accounts in an Organisation using GuardDuty member accounts. Retrieve GuardDuty findings through Amazon CloudWatch events.

Explanation:

Correct Answer: C

Kubernetes protection in Amazon GuardDuty helps to find any suspicious activities in Kubernetes clusters within Amazon Elastic Kubernetes Service (Amazon EKS). To detect any suspicious activities, Amazon GuardDuty monitors Kubernetes logs. In a multi-account environment, where accounts are part of AWS Organisation, only GuardDuty delegated administrators' accounts can enable Kubernetes protection for clusters in all member accounts.

Option A is incorrect as GuardDuty member accounts cannot enable Kubernetes protection in Amazon GuardDuty. Only GuardDuty delegated

administrator's accounts are unable Kubernetes protection for the member accounts.

Option B is incorrect as GuardDuty findings can be retrieved from the GuardDuty console or from Amazon CloudWatch Events. The finding cannot be retrieved from logs stored in the Amazon S3 bucket.

Option D is incorrect as GuardDuty member accounts cannot enable Kubernetes protection in Amazon GuardDuty. Only GuardDuty delegated administrator's account can enable Kubernetes protection for the member accounts.

For more information on Kubernetes protection in Amazon GuardDuty, refer to the following URL,

https://docs.aws.amazon.com/guardduty/latest/ug/kubernetes-protection.html

Domain: Network Design

56. A start-up firm has deployed application servers in multiple VPCs created in the same region. There would be low bandwidth intermittent sync traffic between these servers and existing servers at on-premises data centers. You have been assigned to deploy low-cost quick solutions to establish this connectivity with the least admin work.

Which solution can be suggested to meet this requirement?

A>Create a single AWS Managed VPN connection terminating on AWS Transit Gateway attached to multiple VPCs.
B> Create multiple AWS Managed VPN connections terminating on AWS Transit Gateway attached to multiple VGW.
C> Create multiple AWS Managed VPN connections from the on-premises data center to a Virtual private gateway attached to each VPC.
D> Create a single AWS Managed VPN connection over AWS Direct Connect terminating on AWS Transit Gateway.

Explanation:

Correct Answer: A

AWS Transit Gateway is a highly available managed solution that can be used to connect to multiple VPCs. When there is a need to deploy low bandwidth connectivity from on-premises to AWS quickly, AWS managed VPN connection can be used. By terminating AWS managed VPN connection on AWS Transit Gateway, it will be able to connect to multiple VPCs. With this solution, cost & management for multiple VPN connections can be avoided.

Option B is incorrect as creating multiple VPNs is not required to be terminated on AWS Transit Gateway to connect to multiple VPCs. A single VPN connection terminated on AWS Transit Gateway can have connectivity with

multiple VPCs. **Option C is incorrect** as creating multiple VPN connections will lead to additional costs & management. **Option D is incorrect** as deploying AWS Direct Connect connectivity between on-premises and AWS will require time and cannot be set up quickly.

For more information on hybrid connectivity with AWS Transit Gateway and VPN, refer to the following URL,

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html

Question 37 of 65 Domain: Network Security, Compliance, and Governance

57. A finance company has deployed new application servers in multiple VPCs across multiple availability zones. These servers will be used for critical financial transactions. The security team is concerned about the DNS exfiltration of data moving out of the VPC. As an AWS expert, you have to propose a data filtering solution that will help in preventing this issue.

Which of the following rules can be set up to filter this traffic?

A> Use WAF rules to filter outbound traffic from the VPC.
B> Use NACL to filter outbound traffic from the VPC.
C> Use AWS Network firewall to filter outbound traffic from the VPC.
D> Use Route 53 Resolver DNS Firewall to filter outbound traffic from the VPC.

Explanation:

Correct Answer: D

Route 53 Resolver DNS Firewall can be used to filter DNS traffic from VPC. Filtering rules can be created in the DNS firewall rules group & associate rules group to VPC which can control DNS traffic out of the VPC. This can be used to prevent DNS exfiltration of data which causes a bad actor to control instances within a VPC and uses DNS lookup to send data to a VPC that is under their control.

Option A is incorrect as WAF rules cannot be used to filter DNS traffic outbound from the VPC. **Option B is incorrect** as DNS query traffic from or to the Amazon DNS cannot be filtered using NACL or a security group. **Option C is incorrect** as AWS Network firewall can be used to filter application or network layer traffic, but it cannot be used to filter queries made by Route 53 resolver.

For more information on Route 53 Resolver DNS Firewall, refer to the following URL,

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-dns-firewall.html

Question 38 of 65 Domain: Network Design

58. An engineering firm has hybrid connectivity between on-premises data center & AWS using AWS Direct Connect terminating on Amazon Transit gateway. Amazon EC2 instances are deployed in VPC across multiple availability zones. Interface VPC endpoints are created to establish connectivity from the Amazon EC2 instance to Amazon Kinesis Streams. New servers are deployed at on-premises data centers that require communication with Amazon Kinesis Streams via interface VPC endpoint. As an AWS consultant, you have been assigned to design Amazon Route 53 resolver to establish this connectivity over existing Hybrid connectivity.

What design can be used to achieve this?

A> Disable Private DNS name for VPC endpoint. Create an Amazon Route 53 private Zone using A record pointing to a full service VPC endpoint name. Create an outbound Route 53 resolver endpoint in the same VPC as that of the VPC endpoint. Create conditional forward in the on-premises DNS server for the service name which will point to outbound Route 53 Resolver endpoint IP addresses.

B> Enable Private DNS name for VPC endpoint. Create an Amazon Route 53 private Zone using A record pointing to a full service VPC endpoint name. Create an inbound Route 53 resolver endpoint in the same VPC as that of the VPC endpoint. Create conditional forward in the on- premises DNS server for the service name which will point to inbound Route 53 Resolver endpoint IP addresses.

C> Disable Private DNS name for VPC endpoint. Create an Amazon Route 53 private Zone using Alias record pointing to full service VPC endpoint name. Create an inbound Route 53 resolver endpoint in the same VPC as that of the VPC endpoint. Create conditional forward in the on-premises DNS server for the service name which will point to inbound Route 53 Resolver endpoint IP addresses.

D> Enable Private DNS name for VPC endpoint. Create an Amazon Route 53 private Zone using Alias record pointing to full service VPC endpoint name. Create an outbound Route 53 resolver endpoint in the same VPC as that of the VPC endpoint. Create conditional forward in the on-premises DNS server for the service name which will point to outbound Route 53 Resolver endpoint IP addresses.

Explanation:

Correct Answer: C

For sharing the VPC endpoint with on-premises, the following setting needs to be done.

i) Disable Private DNS name for VPC endpoint: If a private DNS name is enabled, AWS will create a managed private hosted zone that is not accessible from an on-premises network.

ii) Create an Amazon Route 53 private Zone using an Alias record pointing to the full service VPC endpoint name - A custom private zone must be created pointing to the VPC endpoint name.
iii) Create an inbound Route 53 resolver endpoint in the same VPC as that of the VPC endpoint - This inbound endpoint will allow DNS queries from the on-premises DNS server to the VPC endpoint.
iv) Create conditional forward in the on-premises DNS server for the service name which will point to inbound Route 53 Resolver endpoint IP addresses - This will be required for forwarding traffic with the destination as a public hosted zone to inbound Route 53 Resolver endpoint IP addresses.

Option A is incorrect as Amazon Route 53 private zone should be created with alias records pointing to the VPC endpoint name & not A record. Also, an inbound route 52 resolver endpoint should be created to access this private hosted zone, not an outbound resolver endpoint.

Option B is incorrect as AWS creates a managed Route 53 private hosted zone for the service when the Private DNS name is enabled for the VPC endpoint. This managed private hosted zone is accessible only from within the VPC. For accessing this private hosted zone from outside of the VPC, a custom private hosted zone needs to be created & Private hosted zone (PHZ) sharing must be enabled. While accessing from an on-premises location, the inbound Route 53 Resolver endpoint needs to be created in the same VPC.

Option D is incorrect as AWS creates a managed Route 53 private hosted zone for the service when the Private DNS name is enabled for the VPC endpoint. This managed private hosted zone is accessible only from within the VPC. For accessing this private hosted zone from outside of the VPC, a custom private hosted zone needs to be created & Private hosted zone (PHZ) sharing must be enabled. While accessing from an on-premises location, the inbound Route 53 Resolver endpoint needs to be created in the same VPC.

For more information on sharing VPC endpoint from on-premises using Route 53 resolver, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/integrating-aws-transit-gateway-with-aws-privatelink-and-amazon-route-53-resolver/

Domain: Network Implementation

59. A Company has created a VPC with multiple CIDR blocks for deploying applications. The company is using Hybrid connectivity from on-premises locations using AWS Direct Connect. DNS servers are deployed at on-premises locations. Multiple domains are created on-premises which will need access from all VPCs.

What configuration can be done to meet this requirement?

A> Create an outbound endpoint from each VPC. Create a single rule for all domains & associate it with the VPC which will be forwarding queries to the DNS servers deployed at on-premises.

B> Create an outbound endpoint from each VPC. Create separate rules for each domain & associate them with the VPC which will be forwarding queries to the DNS servers deployed at on-premises.

C> Create an inbound endpoint at each VPC. Create separate rules for each domain & associate it with the VPC which will be receiving responses from the DNS servers deployed at on-premises.

D> Create an inbound endpoint at each VPC. Create a single rule for all domains & associate it with the VPC which will be receiving response from the DNS servers deployed at on- premises.

Explanation:
Correct Answer: B
Outbound Endpoints can be used to forward DNS queries to on-premises DNS servers from Amazon EC2 instances in each VPC. Rules are created to specify domain names for which queries are forwarded. Each rule specifies a single domain name; multiple rules need to be created for multiple domain names.

Option A is incorrect. Each rule specifies the domain name of the queries that need to be forwarded to on- premises DNS servers that can support only one domain name. For multiple domain names, multiple rules need to be created.
Option C is incorrect. For forwarding DNS queries from the VPC to an on-premises DNS server, an outbound endpoint needs to be created, not the inbound endpoint.
Option D is incorrect. For forwarding DNS queries from the VPC to an on-premises DNS server, an outbound endpoint needs to be created, not the inbound endpoint.

For more information on outbound endpoints, refer to the following URLS,
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html

Question 40 of 65 Domain: Network Design

60. A company has recently deployed new web applications on Amazon EC2 instances in multiple availability zones with IPv6 addresses. The company is using a third-party DNS provider & needs to point their zone apex record example.com to the Amazon EC2 DNS name. Third-party DNS Providers do not support alias records. Web applications need to be securely accessed globally by a large number of users.

What design pattern can be implemented to meet this requirement in the most cost-effective way?

A> Create a Network Load balancer in each AZ. Create AAAA records for the zone apex pointing to this Network Load Balancer which will, in turn, point traffic to Amazon EC2 instances in each AZ

B> Assign Elastic IP address to the Amazon EC2 instance in different AZs. Create AAAA records for the zone apex pointing to these Elastic IPs.

C> Create an AWS Global Accelerator pointing to the Network Load balancer in each AZ. Create AAAA records for the zone apex pointing to this Network Load Balancer which will, in turn, point traffic to the Amazon EC2 instance in each AZ.

D> Create an AWS Global Accelerator pointing to the Application Load balancer in each AZ. Create AAAA records for the zone apex pointing to this Application Load Balancer which will, in turn, point traffic to the Amazon EC2 instance in each AZ.

Explanation:

Correct Answer: A

Zone Apex (example.com) can be pointed to an IP address & not to a DNS name. In the case of services hosted on AWS, a DNS name is provided. Amazon Route53 supports alias records which can point zone apex to the DNS name used by AWS services. For third-party DNS providers, when alias records are not supported following three alternate design patterns can be used,

a. Using Amazon EC2 instance with Elastic IP address: This will need Amazon EC2 instance to be publicly accessible & is against security best practices.
b. Use AWS Global Accelerator: This is suitable for IPv4 (A records) but does not support IPv6 (AAAA records).
c. Use AWS Network Load Balancer: AWS Network Load Balancer can be deployed in each Availability Zone. AWS NLB gets a static IP address from each Availability zone. Third-party DNS providers can point zone apex (example.com) to these static IP addresses. NLB will load balance traffic to Amazon EC2 instances deployed in private subnets of the VPC. This will ensure Amazon EC2 instances are not publicly accessible & also AWS NLB can handle millions of requests without any service impact.

Option B is incorrect. For this solution to work, Amazon EC2 instances will be publicly accessible. This may lead to additional security risk & further protection needs to be added to publicly accessible Amazon EC2 instances.

Option C is incorrect as with AWS Global Accelerator, additional charges will be incurred.

Option D is incorrect as with AWS Global Accelerator, additional charges will be incurred.

For more information on pointing apex records to AWS service in the case of third-party DNS providers, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/solving-dns-zone-apex-challenges-with-third-party-dns-providers-using-aws/

Question 41 of 65 Domain: Network Management and Operation

61. A large company has deployed a couple of applications in a VPC. Multiple accounts within the company have been created in different VPCs. Account A has created VPC A while account B has created VPC B. A new application will be deployed on an Amazon EC2 instance in VPC A which will communicate with servers in all other VPCs. This instance will be front-ended by a Network Load Balancer. During the POC of the application, all the traffic should be captured and sent to an Amazon EC2 instance launched in VPC B.

What configuration needs to be done to get these packet details?

A> Enable traffic mirroring from the ENI (Elastic Network Interface) and send mirrored traffic to ENI of the Amazon EC2 instance part of VPC B. Create traffic mirror filter rules to match source and destination CIDR block. Enable VPC peering between VPC A and VPC B.

B> Enable traffic mirroring from the IP address assigned to the primary ENI of the Amazon EC2 instance and send mirrored traffic to another ENI of the Amazon EC2 instance. Create a traffic mirror filter rules to match the interface ID of the source and destination Amazon EC2 instance. Enable VPC sharing between VPC A and VPC B.

C> Enable traffic mirroring from the IP address of the Network Load Balancer and send mirrored traffic to another ENI of the Amazon EC2 instance. Create traffic mirror filter rules to match source and destination CIDR blocks. Enable VPC sharing between VPC A and VPC B.

D> Enable traffic mirroring from the IP address of the Network Load Balancer and send mirrored traffic to another ENI of the Amazon EC2 instance. Create a traffic mirror filter rules to match the interface ID of the source and destination Amazon EC2 instance. Enable VPC peering between VPC A and VPC B.

For VPC Traffic Mirroring, the following source and target are supported,

1. Source: Elastic Network Interface of the Amazon EC2 instance.

2. Target:

i). Elastic Network Interface of the Amazon EC2 instance.

ii). Network Load Balancer with UDP Listener

iii). Gateway Load balancer with UDP Listener

Both Source and Target can be part of the same VPC or a different VPC. Traffic mirror filter rules can be used to define the traffic to be mirrored. The following parameters can be selected,

1) Traffic direction (inbound or outbound)
2) Action (accept or reject the packet)
3) Protocol (L4 protocol)
4) Source port range
5) Destination port range
6) Source CIDR block
7) Destination CIDR block

Since the Source Amazon EC2 instance is part of VPC A and the target Amazon EC2 instance to which mirrored traffic is sent is part of VPC B. VPC peering needs to be configured.

Option B is incorrect as the Source of the Traffic mirroring can only be the ENI of the Amazon EC2 instance and not the IP address assigned to the ENL Traffic Mirror filter rules do not support matching interface id. Since source and target are part of VPC A and VPC B respectively, VPC peering is required, not VPC sharing.

Option C is incorrect as the Source of the Traffic mirroring can only be ENI of the Amazon EC2 instance and not the IP address assigned to the NLB. Since source and target are part of VPC A and VPC B respectively, VPC peering is required, not VPC sharing.

Option D is incorrect as the Source of the Traffic mirroring can only be ENI of the Amazon EC2 instance and not the interface of the NLB. Traffic Mirror filter rules do not support matching interface id.

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-connection.html

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-how-it-works.html

https://docs.aws.amazon.com/vpc/latest/mirroring/traffic-mirroring-connection.html

Question 42 of 65 Domain: Network Security, Compliance, and Governance

62. A company has created multiple AWS accounts for each division, and all these accounts are part of the AWS Organization. Multiple VPCs are created in each of these accounts which host production and non-production environments. A separate VPC is created to launch the NAT gateway, and all internet traffic should flow via this VPC. The company is planning to implement VPC sharing between all these VPCs. The IT team is concerned about the subnets to be planned for the NAT Gateway, and

devices to be launched in production and non-production environments in each of the VPC participants.

Which of the following are the best practices with respect to subnet sharing?

A> Dedicated subnets for NAT Gateway. For production environments, shared subnets between many VPC participants. For non-production environments, separate subnets per VPC participant.

B> Dedicated subnets for NAT Gateway. For production environments, dedicated subnets per VPC participants. For non-production environments, shared subnets with many VPC participants.

C> Shared subnets for NAT Gateway. For production environments, dedicated subnets per VPC participants. For non-production environments, shared subnets with many VPC participants.

D> Shared subnets for NAT Gateway. For production environments, shared subnets between many VPC participants. For non-production environments, shared subnets with many VPC participants.

Explanation:

Correct Answer: B

In VPC sharing, subnets are created in the VPC owner account and shared with VPC participants who are part of different AWS accounts in an AWS Organization. While implementing VPC sharing, the following points need to be considered,

1) AWS Infrastructure devices like VPC interface endpoints, firewall endpoints, and NAT gateways should be part of a dedicated subnet. These subnets should not be shared with VPC participants and should only belong to the VPC owner.
2) For production environments, a dedicated subnet needs to be shared with each VPC participant. This will reduce the blast radius of the production subnets in each of the participants' VPCs.
3) For non-production environments, shared subnets may be created to increase IP allocation efficiency.

Option A is incorrect as for production environments dedicated subnets should be used per VPC participants.

Option C is incorrect as AWS Infrastructure devices like VPC interface endpoints, firewall endpoints, and NAT gateways should be part of dedicated subnets and not in shared subnets.

Option D is incorrect as AWS Infrastructure devices like VPC interface endpoints, firewall endpoints, and NAT gateways should be part of dedicated subnets and not in shared subnets. For production environments too, dedicated subnets should be used per VPC participants.

For more information on VPC sharing, refer to the following URL,

https://aws.amazon.com/blogs/networking-and-content-delivery/vpc-sharing-key-considerations-and-best-practices/

Question 43 of 65 Domain: Network Security, Compliance, and Governance

63. A financial company has created two subnets A and B in a VPC. They have deployed servers in each of these subnets. The security team needs to inspect traffic flowing between these servers in subnet A and B using a third-party firewall appliance installed on the separate Amazon EC2 instance. You are assigned to configure necessary routing to ensure all traffic between subnet A and subnet B is via firewall appliance.

What changes can be implemented to get this routing done efficiently?

A> Configure firewall appliance in an Amazon EC2 instance in a subnet B of a VPC. Manually create routing tables for all the subnets in a VPC.
B> Configure firewall appliance in an Amazon EC2 instance in a subnet A of a VPC. Use Middlebox routing wizard to create routing tables.
C> Configure firewall appliance in an Amazon EC2 instance in a separate subnet. Use Middlebox routing wizard to create routing tables.
D> Configure firewall appliance in an Amazon EC2 instance in a separate subnet. Manually create routing tables for all the subnets in a VPC.

Explanation:
Correct Answer: C

Middlebox Routing configures fine-grain control over the routing path for traffic within a VPC. It can be used to redirect traffic for the following purpose,

i. Inspect all traffic destined for a subnet.
ii. Security appliances behind a Gateway Load Balancer in the security VPC.
iii. Inspect traffic between subnets of a VPC.
iv. Multiple middleboxes in the same VPC.

Middlebox Routing will help to build routing tables automatically and hops to redirect traffic between two subnets in a VPC to a security appliance for traffic inspection. The firewall Appliance used for traffic inspection should be part of a separate subnet and should not belong to the subnet for which traffic must be inspected.
Option A is incorrect as Firewall Appliance should be part of a separate subnet than the subnets between traffic is to be inspected. Manual routing for traffic redirection is not an efficient way of creating a route table.
Option B is incorrect as Firewall Appliance should be part of a separate subnet than the subnets between traffic is to be inspected.

Option D is incorrect as Manual routing for traffic redirection is not an efficient way of creating a route table.

For more information on Middlebox Routing, refer to the following URLS
https://docs.aws.amazon.com/vpc/latest/userguide/intra-vpc-route.html
https://docs.aws.amazon.com/vpc/latest/userguide/middlebox-routing-console.html

Question 44 of 65 Domain: Network Design

64. The IT company has set up three-tier web servers in VPC A and VPC B. For communication between VPCs, they are using the AWS Transit gateway. They have created a Local Zone to deploy application servers closer to end-users. For this, they have created a new subnet in VPC A and extended it to the Local Zone. The project team has additional requirements to connect subnets in the Local Zone to subnets in VPC B.

What configuration can be done to establish this connectivity?

A> Create a Transit gateway attachments for VPCA and VPC B using Local Zone subnets in VPC A. In VPC B, add an entry in the routing table for the destination Local Zone A subnet with the target as the network interface id of the transit gateway attachment.

B> Create a Transit gateway attachments for VPC A and VPC B using the parent Availability Zone subnets. In the local zone A, add an entry in the routing table for the destination VPC B subnet with the target as the network interface id of the transit gateway attachment

C> Create a Transit gateway attachments for VPC A and VPC B using Local Zone A subnets. In the local zone A, add an entry in the routing table for the destination VPC B subnet with the target as the network interface id of the transit gateway attachment.

D> Create a Transit gateway attachment for VPC A and VPC B using parent Availability Zone subnets. In each VPC, add an entry in the routing table for the destination as another VPC CIDR with the target as the network interface id of the transit gateway attachment.

Explanation:
Correct Answer: D

A Transit Gateway Attachment cannot be created for Local Zone subnets.
The following configuration can be done to establish connectivity from Local Zone subnets to subnets in another VPC.

i. Create a Transit Gateway Attachments for parent availability zone subnets. In the above case, it would be for VPC A and VPC B parent availability zone subnets.
ii. In each VPC routing table, add a route for the destination VPC subnet with a target of Transit Gateway attachment.

Route entries will be as shown below,

VPC-A Route Table

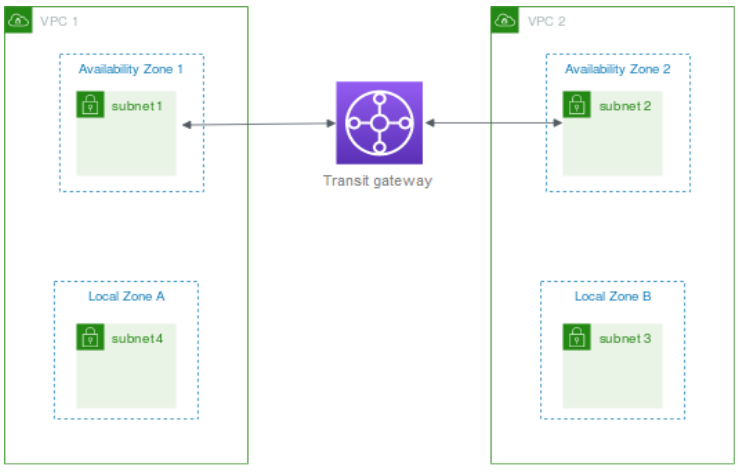
Destination	Target
VPC A CIDR	Local
VPC B CIDR	VPC A -attachment-network-interface-id

VPC-B Route Table

Destination	Target
VPC B CIDR	Local
VPC A CIDR	VPC B -attachment-network-interface-id

Transit Gateway Route Table

CIDR	Attachment	Route Type
VPC A CIDR	Attachment for VPC-A	Propagated
VPC B CIDR	Attachment for VPC-B	Propagated



Option A is incorrect as transit gateway attachments cannot be created for subnets in a Local Zone.
Option B is incorrect as the route table needs to be modified for the VPC, not for the Local Zone.
Option C is incorrect as transit gateway attachments cannot be created for subnets in a Local Zone.

For more information on connecting Local Zone subnets to Transit Gateway, refer to the following URL,
https://docs.aws.amazon.com/vpc/latest/userguide/Extend_VPCs.html#local-zone

Question 45 of 65 Domain: Network Management and Operation

65. A media company is using Amazon CloudFront for distributing content to global users. Recently they have launched a new content for which the Quality Analysis team is looking for requests made to the distribution to analyse responses. The Quality Analysis team is specifically looking for the total number of bytes sent to the viewers in response to the request. These requests should be logged as soon as the requests are received from the users.

Which steps can be initiated to get the required logs?

A> Create a standard log matching sc-bytes and send the logs to the Amazon S3 bucket.
B> Create a real-time log matching sc-bytes and send the logs to the Amazon S3 bucket.
C> Create a standard log matching sc-bytes and send the logs to data streams in the Amazon Kinesis Data Streams.
D> Create a real-time log matching sc-bytes and send the logs to data streams in the Amazon Kinesis Data Streams.

Explanation:

Correct Answer: D

CloudFront real-time logs can be used to capture requests made in real-time and are delivered to the selected data streams of the Amazon Kinesis Data Streams. For real-time logs, any specific fields can be captured. The sc-bytes field captures the total number of bytes sent by the server to the viewer in response to the request. Since the Quality Analysis team is looking to capture response as soon as the requests are made, CloudFront Real-Time logs can provide the details with matching sc-bytes field delivered to Kinesis data streams.

Option A is incorrect as real-time logs should be used since the request logs should be captured as soon as requests are received from the users. **Option B is incorrect** as real-time logs are delivered to Amazon Kinesis Data Streams, not to the Amazon S3 bucket. **Option C is incorrect** as real-time logs should be used since the request logs should be captured as soon as requests are received from the users.

For more information on real-time logs with Amazon CloudFront, refer to the following URL

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/real-time-logs.html

Question 46 of 65 Domain: Network Implementation

66.An online sports network has deployed an application for sharing sports media on an Amazon EC2 instance in the eu- west-2 (London) region. Amazon CloudFront will be used to distribute this content to global users. The IT team plans to use a custom domain name for this distribution. During testing, users are getting domain-name-

related certificate warnings. As an AWS SME, you have been assigned to work on the resolution of this warning.

Which additional settings can be proposed to provide resolution?

A> Select the default SSL/TLS certificate in the Amazon CloudFront and assign it to the custom hostname of the distribution.
B> Request a public SSL/TLS certificate from AWS Certificate Manager in the EU-west-2 (London) region.
C> Request a public SSL/TLS certificate from AWS Certificate Manager in the US east (N. Virginia) region.
D> Import an SSL/TLS certificate with a key length greater than 2048 bits into AWS Certificate Manager in the EU-west-2 (London) region.
E> Import an SSL/TLS certificate with a key length less than 2048 bits into AWS Certificate Manager in the US east (N. Virginia) region.

Explanation:

Correct Answers: C and E

Amazon CloudFront assigns a default SSL/TLS certificate for the default hostname it uses for the distribution. In the case of a non-default hostname for the distribution name, either of the following settings can be done,

1. Request a public certificate from the AWS Certificate Manager.

I). Certificates must be requested in the US east (N. Virginia) region.

II). Appropriate permissions should be granted to use and request certificates from AWS Certificate Manager.

2. Import an SSL/TLS certificate into AWS Certificate Manager

I). Certificates must be imported in the US east (N. Virginia) region.

II). Appropriate permissions should be granted to use and request certificates from AWS Certificate Manager.

III). Key Length of the imported certificate should be between 1024-2048 bits and should not exceed more than 2048 bits.

Once the certificate is requested or imported in the US east (N. Virginia) region, Amazon Cloud Front propagates these certificates to all the edge locations across the globe.

Option A is incorrect as Amazon CloudFront uses the default SSL/TLS certificate for the default hostname of the distribution. This would not work for the custom hostname assigned to the distribution. **Option B is incorrect** as while requesting a public certificate from the AWS Certificate Manager, it must be requested in the US east (N. Virginia) region and not in EU-west-2 (London)

region. **Option D is incorrect** as the key length should be less than 2048 bits while importing an SSL/TLS certificate.

https://aws.amazon.com/premiumsupport/knowledge-center/install-ssl-cloudfront/

https://docs.aws.amazon.com/acm/latest/userguide/gs-acm-request-public.html

https://docs.aws.amazon.com/acm/latest/userguide/import-certificate.html

Question 47 of 65 Domain: Network Implementation

67. An online streaming service provider has deployed a new set of origin servers behind an Amazon CloudFront. Before going to production, the IT Head is looking for a performance test to ensure end-users get better performance while viewing. Tests should ensure that no lag is observed for large scale global users concurrently accessing the content in the production environment.

What testing methodology can be used to test performance?

A> Clients should send requests from a single geographical region.
B>Clients should send requests from multiple geographical regions.
C> Configure the Origin servers with Origin Shield.
D> Clients should connect to a single DNS server which will distribute load across multiple CloudFront locations.
E>Clients should make an independent DNS request.

Explanation:

Correct Answers: B and E

Amazon CloudFront is a scalable service designed for viewers accessing different IP addresses using different DNS resolvers from multiple geographical locations. For load testing CloudFront following method can be adopted,

1. Make sure the client sends requests from multiple geographical locations.

2. While testing, each client should make an independent DNS request, resulting in receiving & different IP address from the DNS. This will ensure the load is distributed across multiple CloudFront servers in different edge locations.

Option A is incorrect as this traffic will hit only some of the CloudFront edge locations, and performance results would not be accurate.

Option C is incorrect as Load testing cannot be done on Origin servers that have Origin Shield enabled.

Option D is incorrect as the Single DNS server will resolve to a single edge location and will not produce accurate results.

For more information on load testing Amazon CloudFront, refer to the following URL

https://docs.aws.amazon.com/Amazon CloudFront/latest/DeveloperGuide/load-testing.html

Question 48 of 65 Domain: Network Design

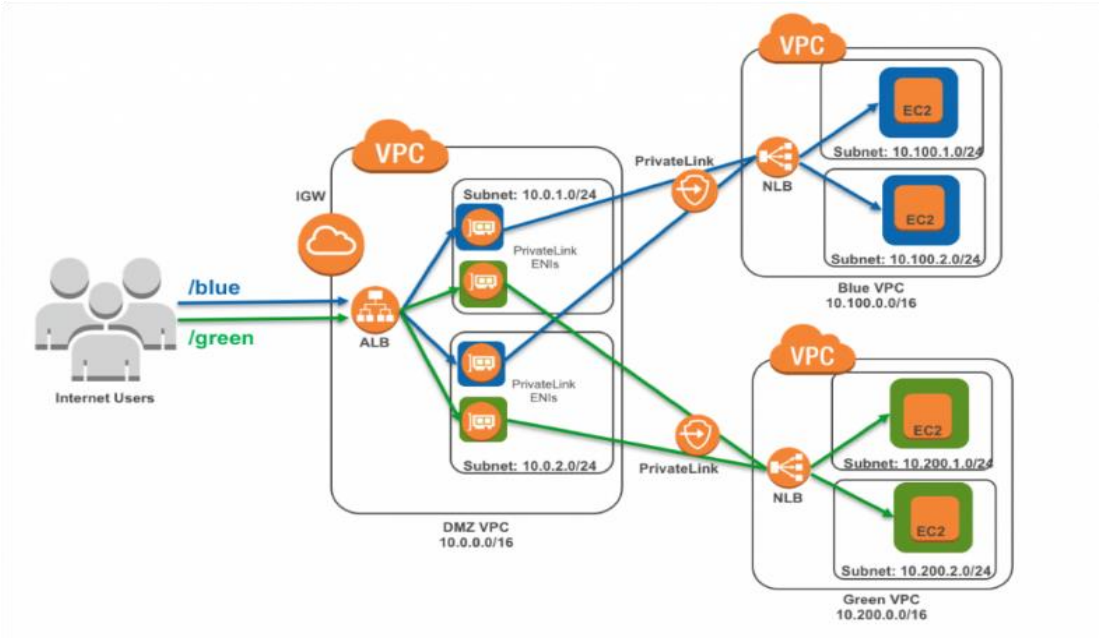
68.A large company is planning to deploy applications in separate VPCs. Each of these applications is accessed by global users via internet connectivity. The IT Head is looking for a solution to provide secure internet connectivity to all these applications with optimum cost and the least management. The proposed solution should allow only HTTP traffic from the internet, and all other traffic should be dropped. Few of the VPCs created have overlapping CIDR ranges. The proposed solution should be scalable with a large number of VPCs created in this account.

What solution can be designed to meet this requirement?

A> Create a separate VPC as "Internet VPC" with Internet gateway and Application Load Balancer. Deploy applications in all other VPCs with Network Load Balancer as the front end. Configure AWS PrivateLink interface in Internet VPC and provide internet access to applications via PrivateLink.
B> Setup a dedicated Internet gateway to each VPC and deploy applications in a public subnet for internet access. Create a Network ACL in each VPC to allow only HTTP traffic and deny all other traffic.
C> Create a separate VPC as "Internet VPC" with an Internet gateway. Deploy a third-party proxy on an Amazon EC2 instance and place it in an Internet VPC. Configure VPC peering between Internet VPC and all other VPCs for internet access to applications.
D> Create a separate VPC as "Internet VPC" with an Internet gateway. Deploy a third-party proxy on an Amazon EC2 instance and place it in an Internet VPC. Configure VPN connectivity between Internet VPC and all other VPCs for internet access to applications.

Explanation:
Correct Answer: A

For providing internet access to multiple VPCS, AWS PrivateLink can be used. In this solution, a separate VPC named "Internet VPC" is created with an Internet gateway attached to it. Applications are deployed in all other VPCs. Between Internet VPC and all other VPCs, a Private Link is created. Private Link ENI is created within the Internet VPC which connects to NLB in each of the VPCS which hosts applications. With this solution, only specific services can be allowed over PrivateLink, making secure connectivity. This can support VPCS with overlapping CIDR ranges. Internet users connect to Application Load Balancer via the Internet gateway. Application Load Balancer forwards the requests to private link ENI to connect to the respective VPC.
The connectivity Diagram can be as follows,



Using PrivateLink in this scenario provides a number of benefits:
The VPC CIDR ranges can overlap between any VPCs. In comparison VPC peering can't be established between VPCs with overlapping IP address ranges.
PrivateLink exposes only the specific service for which it was created: For a web application listening on port 80 (HTTP), the PrivateLink elastic network interface only accepts HTTP connections. No other traffic is allowed from the consumer VPC to the service VPC.
Connections can be initiated only in one direction, from consumer to the service VPC. Applications in the service VPC can't initiate connections to the consumer (DMZ) VPC.
The Internet-facing Application Load Balancer acts as an intelligent reverse proxy, which means there is no need for an additional proxy layer hosted on EC2. The Application Load Balancer should also be combined with AWS Web Application Firewall to protect web applications from common web exploits.

https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-securely-publish-internet-applications-at-scale-using-application-load-balancer-and-aws-privatelink/

Question 49 of 65 Domain: Network Management and Operation

69. A Start-up firm is using an internet-facing application deployed in a VPC. The company uses a Gateway Load Balancer to forward all inbound internet traffic to a pair of firewalls for intrusion detection. It is observed that TCP flow is getting disconnected, and a new session flow is created to different firewalls. Due to this, intermittent timeouts are observed at the client end. Further analysis found that sessions are getting disconnected from Gateway Load Balancer. As an AWS

consultant, you have been assigned to analyze the flow and suggest timers for the TCP flow.

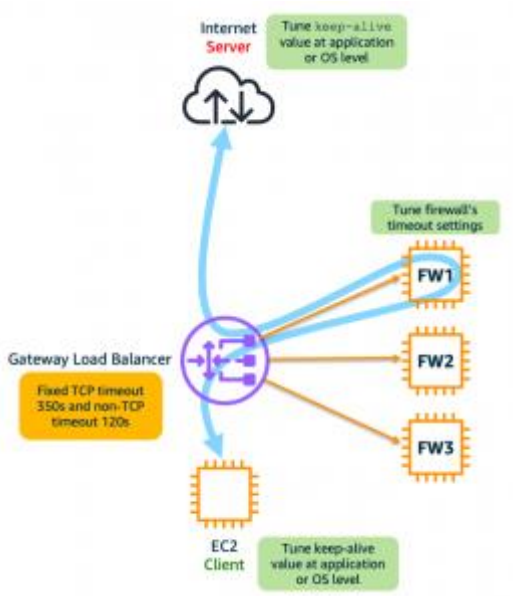
What timers can be set to ensure flow is not removed from Gateway Load Balancer?

A> Set the firewall keep-alive timers to less than 3600 seconds.
B>Set the firewall keep-alive timers to less than 350 seconds.
C> Set the Gateway Load Balancer idle timeout value to 3600 seconds.
D> Set the Gateway Load Balancer idle timeout value to 350 seconds.

Explanation:

Correct Answer: B

Gateway Load Balancer has a fixed idle timeout of 350 seconds for TCP flows and 120 seconds for UDP traffic. To avoid broken TCP sessions between Gateway Load Balancer and the firewall, keep alive timers in the firewall to a lower value than the idle timers at the Gateway Load Balancer. 'Keep alive timers' can be set at the client OS level or in the firewall. Keep Alive Timers can be set in less than 350 seconds for TCP flows and less than 120 seconds for UDP flows.



Option A is incorrect as Firewall Keep-alive timers should be set to less than the idle timeout values of the gateway load balancer which is 350 seconds.

Option C is incorrect as Gateway Load Balancer has a fixed idle timeout value for TCP as 350 seconds, and it cannot be changed.

Option D is incorrect as Gateway Load Balancer has a fixed idle timeout value for TCP as 350 seconds, and it cannot be changed.

For more information on best practices while configuring Gateway Load Balancer, refer to the following URL

https://aws.amazon.com/blogs/networking-and-content-delivery/best-practices-for-deploying-gateway-load-balancer/

Domain: Network Management and Operation

69. An IT company has deployed application servers on Amazon EC2 instances in multiple VPCs. A third-party firewall appliance is deployed in a separate VPC. All Traffic between source and destination Amazon EC2 instance is transparently forwarded to this appliance via Gateway Load balancer endpoint. Firewall Appliance and the Gateway Load balancer use Geneve protocol for traffic exchange. The Operations Team is concerned with the health checks between the Gateway Load Balancer and the appliance.

Which of the following settings will ensure the appliance successfully responds to the health checks from the Gateway load Balancer?

A> Respond to TCP/UDP health checks from Gateway Load Balancer with Geneve encapsulated packets.
B> Respond to TCP/UDP health checks from Gateway Load Balancer from both control and data plane.
C> Respond to TCP/HTTP/HTTPS health checks from Gateway Load Balancer by finishing these checks within timeouts.
D> Respond to TCP/HTTP/HTTPS health checks from Gateway Load Balancer from the data plane.

Explanation:

Correct Answer: C

Gateway Load Balancer periodically sends TCP/HTTP/HTTPS packets to the appliance for health checks. The appliance should respond to these packets as below,

1) TCP: For establishing a connection between the appliance and Gateway Load Balancer.
2) HTTP: for HTTP requests sent by the Gateway Load balancer over a new TCP connection, appliances should respond to status codes between 200 to 399. For all other status codes, Health checks fail.
3) HTTPS: These packets are responded similarly to that of HTTP. The Gateway Load balancer does not perform any hostname verification on the certificate. So, any valid certificate passes the health checks.

All these checks should be finished before the Gateway Load Balancer timeouts. Health checks are done only for control plane traffic with an assumption that the appliance will respond to data plane packets similarly to control plane packets.

Option A is incorrect as health check packets are not required to be sent in Geneve encapsulated format. **Option B is incorrect** as appliances should respond to TCP/HTTP and HTTPS packets, not TCP/UDP. Appliances should respond from the control plane. **Option D is incorrect** as for health checks to

be successful, appliances should respond from the control plane and not from the data plane.

For more information on Gateway Load Balancer health checks, refer to the following URL

https://aws.amazon.com/blogs/networking-and-content-delivery/integrate-your-custom-logic-or-appliance-with-aws-gateway-load-balancer/

Domain: Network Implementation

70. An IT company has set up a hybrid connectivity between AWS cloud and data center. They have set up a Route 53 private hosted zone in the AWS and have an existing DNS server in the data center. Route 53 resolver endpoint is configured to forward all queries for the domain example.com to the DNS server in the data center. Recently they have created a subdomain test.example.com in the AWS cloud. Queries for this subdomain to be resolved by the resolver and should not be forwarded to the DNS server in the data center.

What rules can be configured to get DNS resolution as per requirement?

A> Create a recursive rule specifying test.example.com
B> Create a conditional forwarding rule specifying test.example.com
C> Create a conditional forwarding rule specifying test.example.com disabling an auto defined rule.
D> Create a System rule and specify test.example.com

Explanation:

Correct Answer: D

Rules for Route 53 Resolver endpoints are categorized in two ways,

1. Who creates the rules,

a) Auto defined Rules: These rules are automatically created by the resolver and are associated with the VPC.
b) Custom Rules: These rules are created by the customer.

2. What rules do,

a) Conditional Forwarding Rules: These rules are created to forward DNS queries for a specific domain name to the DNS server on the on-premises.
b) System Rules: These rules are created to override the domain names in the conditional forwarding rule selectively. With Conditional forwarding rules, all the queries for the domain name are forwarded to on-premises DNS servers. If queries need to be handled by the resolver for a sub-domain, system rules can be created for that sub-domain. In the above case, all queries for domain example.com are forwarded to the DNS server. For sub-domain

test.example.com, a system rule can be created so that queries for that sub-domain will not be forwarded to the DNS server in the data center.

c) Recursive Rules: Resolver automatically creates a recursive rule for all domains which are not part of the custom rules or are not defined in the auto-defined rules.

Option A is incorrect as the recursive rule will not be useful for selectively overriding forwarding rules. **Option B is incorrect** as with conditional forwarding rules, queries for the domain name specified will be forward to the DNS server on-premises. **Option C is incorrect** as with conditional forwarding rules, queries for the domain name specified will be forward to the DNS server on-premises. Conditional Forwarding rules (forwarding rules) are part of custom rules which users can specify. These rules are not created automatically by the resolver as in auto-defined rules.

Domain: Network Implementation

71. A company uses hybrid connectivity between data centers and AWS using AWS Direct Connect. The DNS server in the data center is forwarding DNS queries to VPC using an inbound Resolver endpoint. A new application will be deployed in the VPC. The operations team expects high growth in DNS queries due to deploying a new application in the VPC.

Which additional configuration can be done proactively to ensure DNS queries are successfully resolved?

A> Add more IP addresses to the inbound Resolver endpoint in a different Availability Zone.

B> Add additional inbound Resolver endpoints and attach to different Availability Zone.

C> Add additional inbound Resolver endpoint and attach to the same Availability Zone.

D> Add more IP addresses to the inbound Resolver endpoint in the same Availability Zone.

Explanation:

Correct Answer: A

The Route 53 resolver endpoint currently supports 10,000 queries per second per IP address. In case of increasing queries per second, an additional IP address per Resolver endpoint can be added. There is a soft limit of 6 IP addresses per resolver endpoint.

Option B is incorrect. To resolve a large number of queries per second, a better solution is of adding additional IP addresses to resolver endpoints instead of adding multiple inbound resolver endpoints.

Option C is incorrect. To resolve a large number of queries per second, a better solution is of adding additional IP addresses to resolver endpoints instead of adding multiple inbound resolver endpoints.

Option D is incorrect as IP address should be added in the different Availability Zones instead of assigning IP address in the same Availability Zone.

For more information on Amazon Route53 resolver endpoints, refer to the following URL
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver.html#resolver-considerations-number-of-endpoints

Domain: Network Design

72. A company has created a shared-services VPC for centralized DNS management. IT Team has created private hosted zones in this shared services VPC. Applications are deployed in different Spoke VPCs. Private hosted zone in shared- services VPC needs to be resolved across multiple accounts created in Spoke VPCs. The proposed solution should also be valid for forwarding DNS queries from on-premises to the shared service VPC in the near future.

What connectivity can be proposed to meet this requirement in the most cost-effective manner?

A> Establish network connectivity between shared services VPC and Spoke VPC using AWS Transit Gateway. Use Amazon Route 53 resolver forwarding to query Route 53 private hosted zones from multiple accounts in Spoke VPCs.
B> Establish network connectivity between shared services VPC and Spoke VPC using AWS Transit Gateway. Share the private hosted zone between accounts and associate with the Spoke VPC that needs resolution.
C> Establish network connectivity between shared services VPC and Spoke VPC using VPC peering. Share the private hosted zone between accounts and associate with the Spoke VPC that needs resolution.
D> Establish network connectivity between shared services VPC and Spoke VPC using VPC peering. Use Amazon Route 53 resolver forwarding to query Route 53 private hosted zones from multiple accounts in Spoke VPCs.

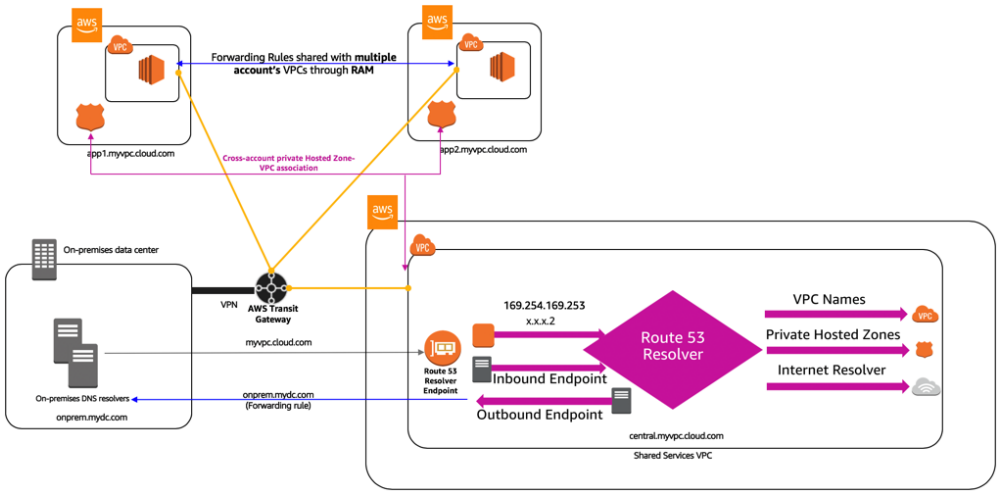
Explanation:
Correct Answer: B

Private Hosted Zones created in a shared-services VPC can be resolved in multiple accounts setup in different Spoke VPCs in the following manner,

I. Interconnect Spoke VPC and the Shared-services VPC by AWS Transit Gateway.
II. Share Private Hosted zone between accounts using AWS RAM and associate it with Spoke VPC that needs resolution.

In case of any future requirements of privately hosted zone resolution from the on-premises network, the On-premises network can be connected to AWS

Transit Gateway, and an inbound Route 53 resolver endpoint can be created in shared services VPC.
Option A is incorrect as using Route 53 resolver forwarding will incur additional costs and introduce complexity in administration.
Option C is incorrect as VPC Peering will not work only with VPC-to-VPC private hosted zone resolution. For forwarding queries from on-premises, a separate setup will be required, resulting in additional cost.
Option D is incorrect as Route 53 resolver forwarding will incur additional costs and introduce complexity in administration. VPC Peering will not work only with VPC-to-VPC private hosted zone resolution. For forwarding queries from on-premises, a separate setup will be required, resulting in additional cost.



https://aws.amazon.com/blogs/networking-and-content-delivery/centralized-dns-management-of-hybrid-cloud-with-amazon-route-53-and-aws-transit-gateway/

Question 54 of 65 Domain: Network Implementation

73. A start-up company is planning to use Amazon Route 53 as a DNS for applications in AWS Cloud Infrastructure. Applications will be deployed in multiple regions catering to local users in each region. While setting Route 53 route policies, the IT team should ensure that queries are responded based on the user's location so that users can access applications from the nearest region. Route policy should respond to the queries in a stable and predictable way. The IT head needs you to ensure customers do not receive "no answer response" from Route 53.

What settings can be implemented to get this resolution in the desired way?

A> Create a multi-answer routing policy. Create a default policy for queries not mapped to any location.
B> Create a latency-based routing policy. Create a default policy for queries not mapped to any location.
C> Create a Geolocation routing policy. Create a default policy for queries not mapped to any location.

D> Create a Geoproximity routing policy. Create a default policy for queries not mapped to any location.

Explanation:
Correct Answer: C

Geolocation routing policy responds to queries based upon user location. All the users based in a particular location will always get the same response with this routing policy. This will ensure a stable and predictable response to the users. Geolocation routing policy works by mapping users' IP addresses to locations. Route 53 responds with a "no answer response" for user's IP addresses that are not mapped to any locations. A default policy needs to be created for all the users which are not mapped to any location so that users do not receive a "no answer response" from Route 53.

Option A is incorrect as with multivalue answer routing policy, the client selects based upon random responses it receives from Route 53. For the multivalue answer policy, no default policy is required to be set.
Option B is incorrect as with latency-based routing, based upon latency, routing data can frequently change which may lead to unpredictable responses to the queries when there is a change in latency.
Option D is incorrect as the Geoproximity routing policy can be used to route traffic based upon resource location and not based upon user locations.

For more information on best practices with Amazon Route53, refer to the following URLS
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/best-practices-dns.html
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html#routing-policy-geo

Question 55 of 65 Domain: Network Design

74. A large engineering firm plans to deploy HPC applications in the AWS cloud for its R&D work. HPC applications will be deployed on Linux-based Amazon EC2 instances. All these instances will be launched in a single subnet of the VPC. Traffic between these instances should have the lowest latency without any impact on the network performance.

Which deployment option will provide optimum performance for HPC applications?

A> Enable enhanced networking on Amazon EC2 instance with Elastic Network Adaptor (ENA). Place all Amazon EC2 instances in a partition placement group.
B> Enable enhanced networking on Amazon EC2 instance with Intel 82599 Virtual Function (VF). Place all Amazon EC2 instances in a cluster placement group.

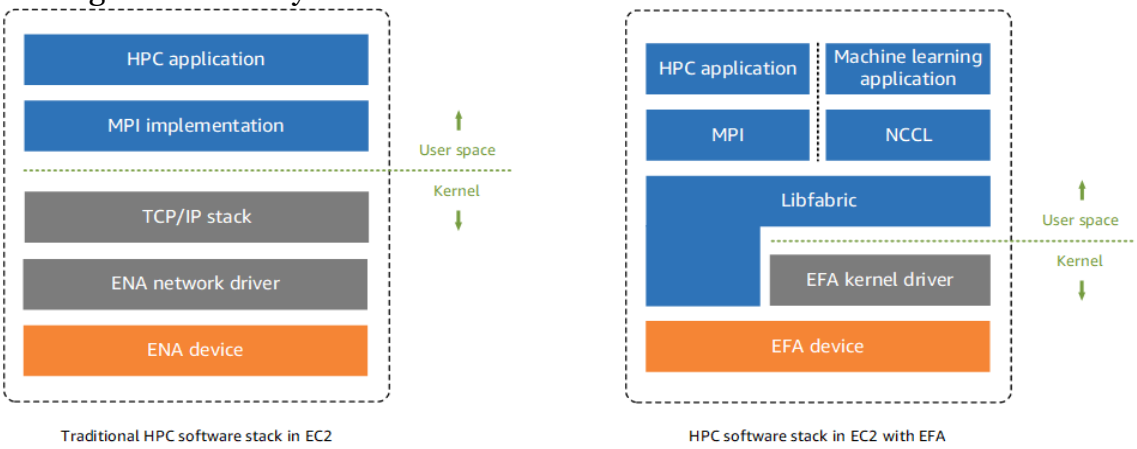
C> Enable enhanced networking on Amazon EC2 instance Elastic Fabric Adaptor (EFA). Place all Amazon EC2 instances in a cluster placement group.

D> Enable enhanced networking on Amazon EC2 instance with Intel 82599 Virtual Function (VF). Place all Amazon EC2 instances in a partition placement group.

Explanation:

Correct Answer: C

For better performance of HPC applications in AWS Cloud, applications should be launched on an Amazon EC2 instance with EFA and launched in a cluster placement group. EFA is an ENA with added capabilities that supports HPC applications to communicate with network interfaces resulting in low-latency reliable connectivity directly. EFA supports OS-bypass. With OS-bypass, HPC applications can directly communicate with the network interface hardware leading to low latency and reliable communications.



Option A is incorrect as for better performance for traffic between Amazon EC2 instances, the instance should be placed in a cluster placement group and not in a partition placement group. For HPC applications, instances with EFA would provide better performance than instances with ENA enabled. This is due to an additional OS- bypass feature that EFA supports.

Option B is incorrect as for HPC applications, the instance with EFA would provide better performance than an instance with an ENA Intel 82599 VF interface. This is due to an additional OS-bypass feature that EFA supports.

Option D is incorrect as for better performance for traffic between Amazon EC2 instances, the instance should be placed in a cluster placement group and not in a partition placement group. For HPC applications, an instance with EFA would provide better performance than an instance with an ENA Intel 82599 VF interface. This is due to an additional OS-bypass feature that EFA supports.

For more information on HPC applications performance enhancements, refer to the following URLS

https://dl.awsstatic.com/whitepapers/Intro_to_HPC_on_AWS.pdf

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/efa.html

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

Question 56 of 65 Domain: Network Design

75.A financial company has created hybrid connectivity using AWS Direct Connect connections. The company uses Direct Connect Gateway with a virtual private gateway to connect different VPCs created in multiple regions. For this, they have created a private virtual interface with dedicated Direct Connect connections. They are looking for VPC to VPC communication along with VPC to on-premises communication using the existing setup. This connectivity should support communication with all future VPCs created in multiple regions.

What configuration changes will be required to establish this connectivity?

A> Remove the association between Direct Connect gateway and virtual private gateway. Create a new private virtual interface and associate Transit Gateway in each region with AWS Direct Connect Gateway using the same BGP ASN for all Transit Gateways.

B> Keep existing association between Direct Connect gateway and virtual private gateway using the virtual private interface. Create a new private virtual interface and associate Transit Gateway in each region with AWS Direct Connect Gateway using a unique BGP ASN for each Transit gateway.

C> Keep existing association between Direct Connect gateway and virtual private gateway using the virtual private interface. Create a new transit virtual interface and associate Transit Gateway in each region with AWS Direct Connect Gateway using the same BGP ASN for all Transit gateways.

D> **Remove the association between Direct Connect gateway and virtual private gateway. Create a new transit virtual interface and associate Transit Gateway in each region with AWS Direct Connect Gateway using a unique BGP ASN for each Transit gateway.**

https://docs.aws.amazon.com/vpc/latest/tgw/tgw-dcg-attachments.html

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

Explanation:

Correct Answer: D

Direct Connect Gateway can be used to connect AWS Transit gateway created in multiple regions. A virtual transit interface is required with AWS Direct Connect for this connectivity. Link bandwidth should be greater than 1Gbps. For connecting Transit Gateway in different regions to Direct Connect Gateway, a unique BGP ASN is

required at each of the Transit Gateways. To associate the Direct Connect gateway with the Transit Gateway, existing associations with the Virtual Private Gateway over the private virtual interface must be removed.

The connectivity Diagram will be as follows,

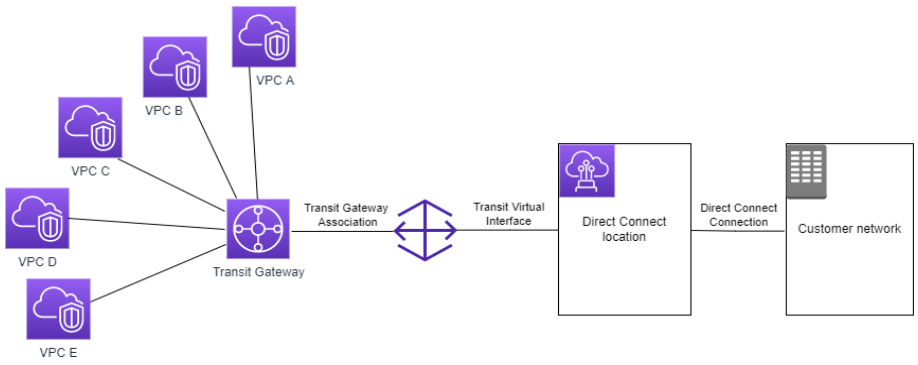


Figure 7 Direct Connect Gateway with Transit Gateway

Option A is incorrect as Direct Connect Gateway cannot be associated with Transit Gateway using a private virtual interface.

Option B is incorrect as Direct Connect Gateway cannot be associated with Transit Gateway using a private virtual interface. Direct Connect Gateway cannot be associated with Transit Gateway when it is already associated with a virtual private gateway.

Option C is incorrect as associating multiple Direct Connect Gateway with AWS Transit Gateway BGP ASN must be different.

Question 57 of 65 Domain: Network Implementation

76. A start-up company is establishing a hybrid connectivity between an on-premises network and AWS using AWS Direct Connect. They have created a Private virtual interface to the Virtual Private gateway. While performing tests,

connectivity is not established from the on-premises network to the VPC. As an AWS Consultant, you have been asked to provide suggestions to troubleshoot this connectivity.

What checks need to be performed to ensure connectivity is properly established from VPC towards on-premises networks?

A> In VPC route tables, add entries for on-premises routes with the target as a virtual private gateway that has a private virtual interface connected.

B> Ensure that not more than 1000 routes are advertised from on-premises customer routers.

C> Ensure that only a default route is advertised from on-premises customer routers.

D> In the VPC route table, disable route propagation for routes from the virtual private gateway.

E> Ensure that no more than 100 routes are advertised from the on-premises customer router.

Explanation:
Correct Answers: A and E

For private virtual interface or transit virtual interface, 100 routes can be advertised per BGP session from an on- premises router to AWS. For a public virtual interface, 1000 routes can be advertised. In the VPC route table, routing can be done in either of the two ways,

i. Enable route propagation which will propagate routes from the on-premises network to the VPC routing table.
ii. Add entries for on-premises routes in the VPC routing table with the target as a virtual private gateway.

Option B is incorrect as for private virtual interfaces only 100, not 1000 BGP routes can be advertised from on- premises customer routers.
Option C is incorrect as it's not necessary to advertise only the default route. Clients can advertise specific routes which are less than 100.
Option D is incorrect as route propagation can be enabled and not disabled for routes from the on-premises network to the VPC route table.

https://docs.aws.amazon.com/directconnect/latest/UserGuide/Troubleshooting.html#ts-routing

Question 58 of 65 Domain: Network Design

77. A company plans to establish hybrid connectivity using AWS Direct Connect dedicated link between on-premises location and AWS. At on-premises, the company has created two VRFs (virtual routing and forwarding) VRF A and VRF B. Servers in VRF A need to have connectivity with CIDR A part of VPC A while server in VRF B needs to have connectivity with CIDR B of VPC B. Both VPC A and VPC B are created in the same AWS region. Routers at the on-premises location do not support GRE (Generic Routing Encapsulation). Traffic from respective VRFS should be end-to-end segmented over AWS Direct Connect connection.

Which of the following can be implemented for segmenting traffic in the most cost-effective way?

A> Create two public VIF over AWS Direct Connect Dedicated connection. Create two Site-to- Site VPN connections from on-premises routers to two different AWS Transit gateway. Each Site-to-Site VPN connection should be part of each VRF A and B created at on-premises location. Create VPC attachments each from VPC A and VPC B to each of the two AWS Transit Gateway. Create route tables in each AWS Transit Gateway for traffic flow between VPC A-VRF A and VPC B-VRF B

B> Create two public VIF over AWS Direct Connect Dedicated connection. Create two Site-to- Site VPN connections from on-

premises routers to the AWS Transit Gateway. Each Site-to- Site VPN connection should be part of each VRF A and B created at the on-premises location. Create two VPC attachments between VPC A and VPC B with the AWS Transit Gateway. Create two separate route tables in AWS Transit Gateway for each traffic flow between VPC A-VRF A and VPC B- VRF B

C> Create a single public VIF over AWS Direct Connect Dedicated connection. Create two Site- to-Site VPN connections from on-premises routers to the AWS Transit gateway. Each Site- to-Site VPN connection should be part of each VRF A and B created at the on-premises location. Create two VPC attachments between VPC A and VPC B with the AWS Transit Gateway. Create single route tables in AWS Transit Gateway for traffic flow between VPC A-VRF A and VPC B- VRF B

D> Create a single public VIF over AWS Direct Connect Dedicated connection. Create a single Site-to- Site VPN connections from on-premises routers to two different AWS Transit gateway. Site- to-Site VPN connection should be part of global VRF in which router leaking from each VRF A and B will be done at on-premises routers. Create two VPC attachments between VPC A and VPC B with AWS transit gateway. Create two separate route tables in AWS transit Gateway for each traffic flow between VPC A- VRF A and VPC B - VRF B

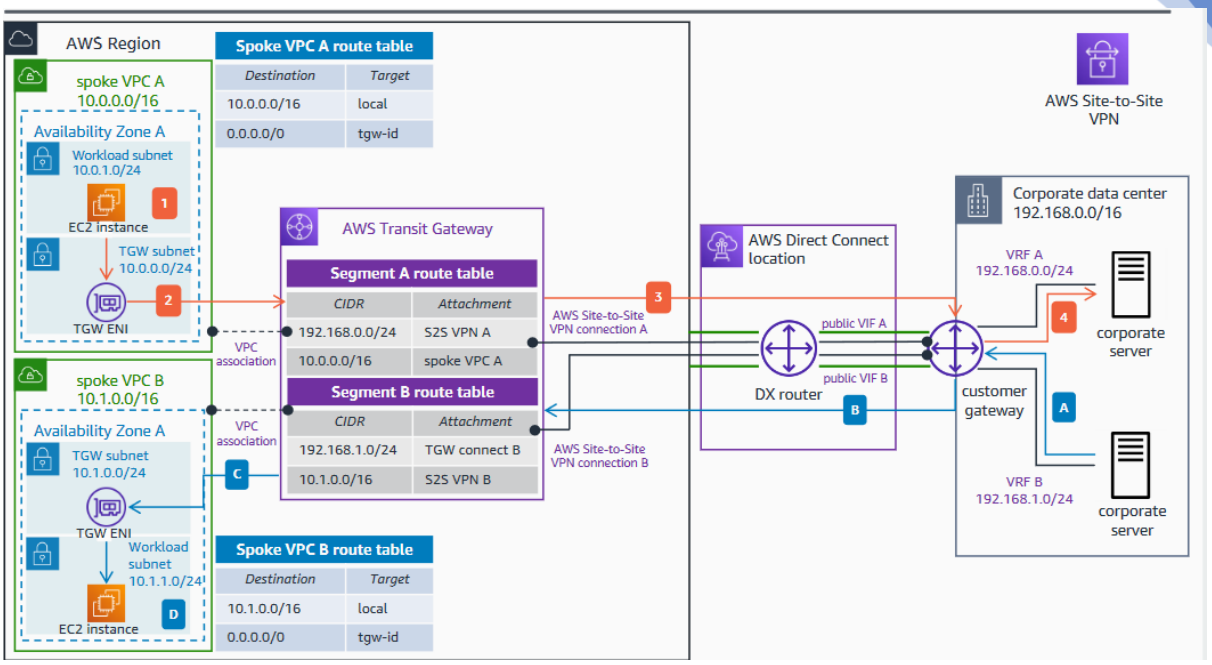
Explanation:

Correct Answer: B

For end-to-end traffic segmentation on non-GRE supporting routers following can be configured,

i. Create two public VIFS over AWS Direct Connect Dedicated connection - Two Public VIFS will be required to create two separate Site-to-Site VPNs on each VIF.
ii. Create two Site-to-Site VPN connections from on-premises routers to the AWS Transit gateway - Each site-to- site VPN will be mapped to two VRFS-VRF A and VRF B at the on-premises.
iii. Each Site-to-Site VPN connection should be part of each VRF A and B created at the on-premises location.
iv. Create two VPC attachments between VPC A and VPC B with the AWS Transit Gateway.
v. Create two route tables in the Transit gateway- One route table for communication between VPCA - VRF A and the other for communication between VPC B and VRF B. In each route table, CIDR will be mapped to VPC attachments and site-to-site VPN attachments for subnets at VPC and on-premises respectively.

The Connectivity Diagram will be as follows,



Option A is incorrect as two AWS Transit gateways are not required for two VPC attachments. This will incur additional costs, and it will be a sub-optimum design. AWS Transit Gateway is a highly available service supporting multiple VPCs attachments.

Option C is incorrect as for segmenting traffic, Site-to-Site VPN needs to be created on two public VIFS, not on a single VIF. In the AWS Transit gateway, separate routing tables should be created for each traffic flow between VPC A-VRF A and VPC B-VRF B.

Option D is incorrect as two Site-to-Site VPNs should be created on two Public VIFS for traffic segmentation. Route-leaking between VRFS is not a recommended solution.

For more information on Segmenting Traffic on AWS Direct Connect, refer to URL

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/traffic-segmentation-aws-direct-connect-ra.pdf?did=wp_card&trk=wp_card

Question 59 of 65 Domain: Network Design

78. A large company is using multiprotocol label switching (MPLS) to connect branch locations across the globe to its data center. They have created multiple VPCs in the AWS cloud and are looking to use existing MPLS connectivity to connect all branches to these VPCs. In the future, the company is planning to expand its presence in the AWS cloud by deploying applications in multiple VPCs. The company requires full

control of network configuration and configuration should be less dependent on the MPLS service provider.

Which option can be implemented to establish a highly available fault-tolerant connectivity?

A> Deploy an MPLS device collocated at the AWS Direct Connect Location and an AWS Direct Connect link to a Transit VPC over which it will connect to multiple VPCs.

B> Deploy an MPLS device collocated at the AWS Direct Connect Location and an AWS Direct Connect link to the Direct Connect gateway connecting to multiple VPCs.

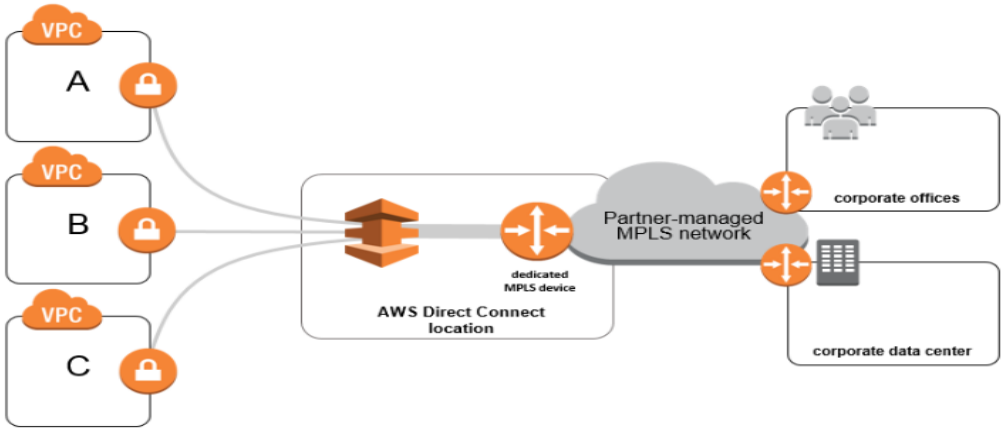
C> Implement connectivity with AWS Direct Connect Location using service-provider managed MPLS network and a hosted AWS Direct Connect connection to VGW attached to each VPC.

D> Implement connectivity with AWS Direct Connect Location using service-provider managed MPLS network and create a VPN connection over single hosted AWS Direct Connect connection to Transit VPC.

Explanation:

Correct Answer: B

Dedicated MPLS devices can be collocated at the AWS Direct Connect location. This will help customers handle network configuration with AWS on their own without any dependency on the service provider. In this option, an MPLS link is implemented between customers' locations and a dedicated router at the AWS Direct Connect location. AWS Direct Connect link is built from this device. To connect multiple VPCs Direct Connect gateway can be used. The Connectivity Diagram is as follows,



Option A is incorrect as with MPLS devices collocated at AWS Direct Connect location, there is no need for additional Transit VPC for connecting to multiple VPCs. All configurations can be done from the dedicated device.
Option C is incorrect as this is not a scalable solution. For each new VPC created in AWS, customers must provide a new hosted connection with the

help of a service provider. This is not suitable for the above case where additional VPC will be created in the future.
Option D is incorrect as this will incur additional designing and maintenance charges for Transit VPC.

For more information on Hybrid Connectivity over MPLS, refer to the following URL
https://do.awsstatic.com/aws-answers/aws-network-connectivity-over-mpls.pdf

Question 60 of 65 Domain: Network Management and Operation

79. A customer is using AWS Client VPN for accessing resources in VPC A from an on-premises network. They are using a split-tunnel Client VPN. Recently, the IT team has created a new VPC B for different applications and established VPC peering between VPC A and VPC B. Users from on-premises can communicate with resources in VPC A but cannot establish connectivity with applications in VPC B.

What changes must be implemented in Client VPN to enable clients to communicate with subnets in peered VPC B?

A> Modify the Client VPN endpoint route table to add a default route. New routes will be automatically propagated to clients.
B> Modify the Client VPN endpoint route table to add a default route. Reset the VPN connection so that new routes are sent to the client.
C> Modify the Client VPN endpoint route table to add a route for peered VPC CIDR range. Reset the VPN connection so that new routes are sent to the client.
D> Modify the Client VPN endpoint route table to add a route for peered VPC CIDR range. New routes will be automatically propagated to clients.

Explanation:

Correct Answer: C

For a client VPN tunnel, by default, all traffic is routed over the client VPN tunnel. If a split-tunnel Client VPN tunnel is used, only traffic for destination routes matching in the Client VPN route table is allowed on the tunnel. When a VPC peering is created, a peered VPC B CIDR range requires to be added in the Client VPN endpoint route table. The default route is not required to be added to the Client VPN endpoint route table. When a split-tunnel is used on a Client VPN endpoint, all the routes in a Client VPN endpoint route table are added to the client route table when a VPN is established. In the above case, since VPC peering is established post creation of the Client VPN, to have VPC subnets advertised to client route tables, connections need to be reset.

Option A is incorrect as the default route is added for the client route table when split-tunnel is not used with the Client VPN endpoint. When a split-tunnel is used

along with the Client VPN endpoint, a specific subnet of the peered VPC CIDR range needs to be added. New subnets are not automatically propagated to client route tables. **Option B is incorrect** as the default route is added for the client route table when split-tunnel is not used with the Client VPN endpoint. When a split-tunnel is used along with the Client VPN endpoint, a specific subnet of the peered VPC CIDR range needs to be added. **Option D is incorrect** as in the case of split-tunnel, new routes are not automatically advertised to the client route table. A connection needs to be reset to propagate these subnets to the client route table.

For more information on routing with Split tunnel enabled on AWS Client VPN, refer to the following URLS,

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/split-tunnel-vpn.html

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/scenario-peered.html

https://docs.aws.amazon.com/vpn/latest/clientvpn-admin/cvpn-working-routes.html#split-tunnel-routes

Question 61 of 65 Domain: Network Implementation

80. A start-up company has implemented hybrid connectivity between on-premises location and AWS using Site-to-Site VPN. Due to the deployment of critical applications in the AWS cloud, they are looking to build redundancy to avoid any failure in connectivity. While implementing this connectivity, there should not be any single point of failure in the end- to-end path. Since there is a financial impact with failure in the application, there are no cost constraints for building additional connectivity.

What can be implemented to ensure end-to-end resiliency for this connectivity?

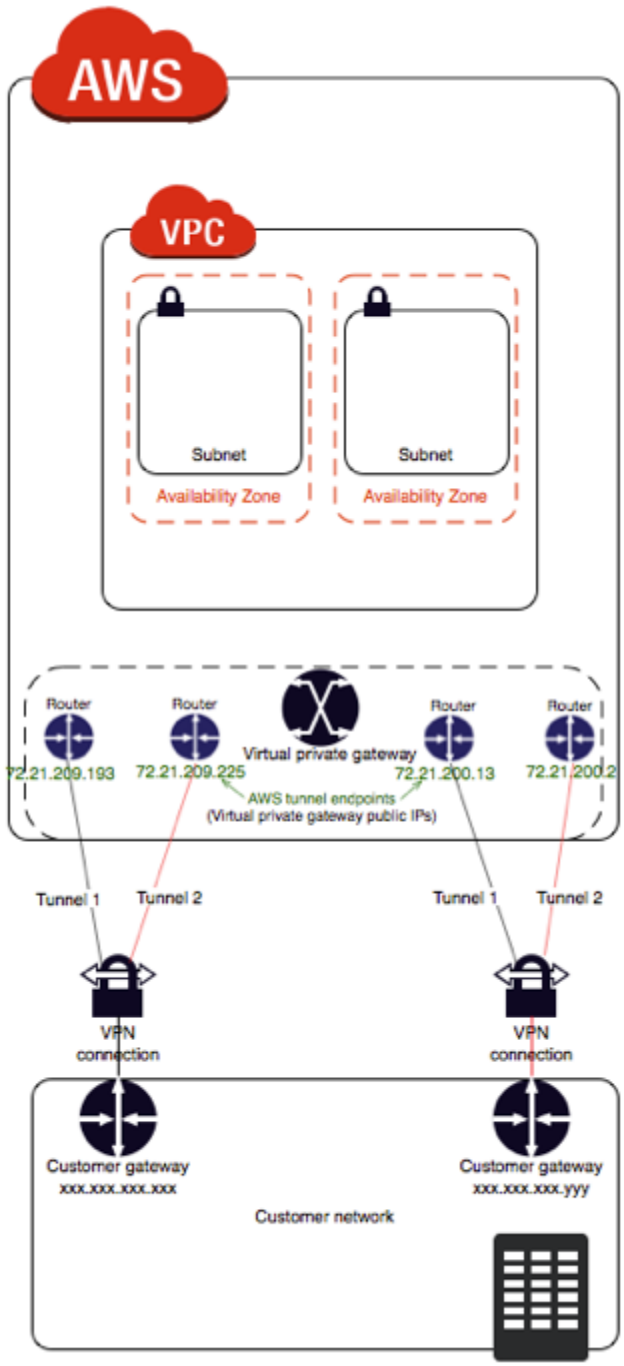
A> Setup a second Site-to-Site VPN on the same VGW. Use the same customer gateway at on- premises. Segregate on-premises prefixes into two pools while advertising from the customer gateway.
B> Setup a second Site-to Site VPN on the different VGW. Use the same customer gateway at on-premises. Segregate on-premises prefixes into two pools while advertising from the customer gateway.
C> Setup a second Site-to Site VPN on the different VGW. Deploy a new customer gateway at on-premises. Advertise on-premises prefixes from both on-premises devices.
D> Setup a second Site-to-Site VPN on the same VGW. Deploy a new customer gateway at on- premises. Advertise on-premises prefixes from both on-premises devices.

Explanation:
Correct Answer: D
For Site-to-Site VPN resiliency following points can be considered,

1. A separate Customer end device can be considered to implement a second Site-to-Site VPN to ensure there is no single point of failure.

2. Same On-Premises prefixes should be advertised from both the customer devices. This will ensure no impact on connectivity in case of failure in one customer end device or a single Site-to-Site VPN.

3. At the AWS end, VGW (virtual private gateway) is a fully managed and redundant device. So, a second Site-to- Site VPN can use the same VGW. A single VGW can be attached to a VPC.



Option A is incorrect as using the same customer gateway will make it a single point of failure. Segregating pools at the client end and advertising to AWS will incur an outage for a pool for which the tunnel is down**. Option B is incorrect** as VGW is an AWS side VPN concentrator that is fully managed, and redundancy is taken care of by AWS. For each VPC, only one VGW can be attached. Using the same customer gateway will make it a single point of failure. Segregating pools at the client end and advertising to AWS will incur an outage for a pool for which the tunnel is down**. Option C is incorrect** as VGW is an AWS side VPN concentrator that is fully managed, and redundancy is taken care of by AWS. For each VPC, only one VGW can be attached.

For more information on redundancy for site-to-site VPN, refer to the following URLS
https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html

https://docs.aws.amazon.com/vpn/latest/s2svpn/your-cgw.html

Question 62 of 65 Domain: Network Design

81. A start-up firm is looking to establish hybrid connectivity from its datacenter to AWS Cloud. VPC A, VPC B, and VPC C are created in the AWS cloud. From the data center, communication should be established with servers deployed in all these VPCs. While setting the connectivity, redundancy and least management overhead should be considered. The proposed connectivity should incur the least operational cost. In a normal scenario, end-to-end traffic should flow only on one of the redundant links.

Which solution can be designed to meet this requirement?

A> Setup two IPsec VPN tunnels from two customer gateway routers to the AWS Transit gateway. Create VPC attachments between all the VPCs and the Transit Gateway. Configure BGP routing to prefer one IPsec VPN tunnel over another.

B> Setup two IPsec VPN tunnels from two customer gateway routers to each of the Virtual Private Gateways attached to all the VPCs. Configure BGP routing to prefer one IPsec VPN tunnel over another.

C> Setup two IPsec VPN tunnels from two customer gateway routers to Virtual Private Gateway attached to the VPC A. Create VPC peering between all the VPCs and VPC A. Configure static routing to prefer one IPsec VPN tunnel over the another.

D> Setup two IPsec VPN tunnels from two customer gateway routers to two AWS Transit gateways. Create VPC attachments from all the VPCs to each of the Transit Gateway. Configure static routing to prefer one IPsec VPN tunnel over another.

Explanation:

Correct Answer: A

An IPsec managed VPC can be used with AWS Transit Gateway to establish connectivity from the on-premises location to multiple VPCs in an AWS Cloud. Creating two IPsec tunnels from two different customer end devices will provide redundancy for this connectivity. BGP policies can be used to make one IPsec VPN tunnel preferred over the other.

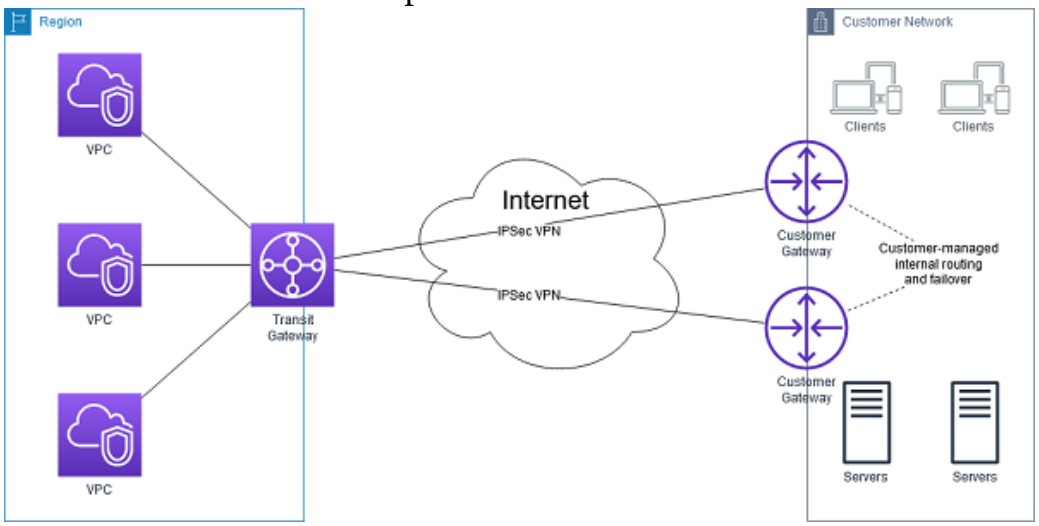


Figure 8 IPsec managed VPC with AWS Transit Gateway

Option B is incorrect as this will incur additional management overhead for managing multiple IPsec VPN tunnels to each of the Amazon VPCs. Also, this will not be a scalable solution. **Option C is incorrect** as Site-to-Site VPN will not work from a VPC over VPC peering. Also, using static routes will lead to additional management overhead. **Option D is incorrect** as AWS Transit Gateway is a highly available and scalable service. It is not necessary to set up two Transit Gateways. Also, using static routes will lead to additional management overhead.

For more information on connectivity with IPsd VPN and AWS Transit Gateway, refer to the following URLS
https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/aws-transit-gateway-vpn.html
https://docs.aws.amazon.com/vpn/latest/s2svpn/vpn-redundant-connection.html

Question 63 of 65 Domain: Network Design

82.A share broking firm is developing a couple of applications for trading. One application will be for share price ticker while the other application will be used for trading. Both these applications will be hosted on Amazon EC2 nitro instance and need multicast support. Recipients of these applications will be a separate ENI (Elastic Network Interface) of instances deployed in the different VPCs. The recipient should only receive multicast traffic from the group to which it has joined. These

instances will be part of multiple VPCs created within a region, and inter-VPC communication will be established using AWS Transit Gateway.

What configuration changes will be required for the application deployment in the VPC and on the Transit gateway for the multicast support?

A> Create applications in single subnets of the VPC CIDR range. Associate this subnet to two different multicast domains created within a transit gateway. Create two different Multicast groups within the Transit gateway.

B> Create applications in single subnets of the VPC CIDR range. Associate this subnet to a single multicast domain created within a transit gateway. Create a single Multicast group within the Transit gateway.

C> Create applications in two separate subnets of the VPC CIDR range. Associate both subnets to two different multicast domains created within a transit gateway. Create two different Multicast groups within the Transit gateway.

D> Create applications in two separate subnets of the VPC CIDR range. Associate both subnets to a single multicast domain created within a transit gateway. Create a single Multicast group within the Transit gateway.

Explanation:
Correct Answer: C

AWS Transit Gateway supports multicast routing between the subnets of the attached VPCs. These subnets act as a multicast router, forwarding multicast traffic from a source instance to multiple receiving instances. A subnet can be part of a single multicast domain. Two separate Multicast groups need to be created for two sets of applications with different sets of sources and receivers in the VPC.
The following are the concept for multicast routing on an AWS Transit Gateway,

1. Multicast Domain: Use for segmentation of multicast networks in different domains. Multicast Domain membership is defined at the subnet level. Transit Gateway acts as a multiple multicast router for domains created.
2. Multicast Group: Set of hosts that will send and receive the same multicast traffic.
3. IGMP: Internet Group management Protocol (IGMP) is used to manage group membership dynamically.
4. Multicast Source: This is an ENI of the supported Amazon EC2 instance that sends traffic.
5. Multicast Group member: This is an ENI of the supported Amazon EC2 instance that receives traffic.

Option A is incorrect as the subnet can be associated with a single multicast domain and not with multiple multicast domains. **Option B is incorrect** as Creating a single domain, and a single multicast group will result in the recipient receiving multicast traffic from both the groups.

Option D is incorrect as Creating a single domain, and a single multicast group will result in the recipient receiving multicast traffic from both the groups.

For more information on multicast routing with AWS Transit Gateway, refer to the following URL
https://docs.aws.amazon.com/vpc/latest/tgw/tgw-multicast-overview.html

Question 64 of 65 Domain: Network Design

83. A global company has created VPCs in multiple regions for deploying applications. They are looking to integrate all these applications to provide scalable solutions to global users. Connectivity should use AWS-managed network infrastructure and should not traverse over the public internet. It should be scalable and support an additional large number of VPCs created in multiple regions.

Which of the following suits the company's needs the best?

A> Connect multiple VPCs to AWS Transit Gateway. Use AWS Transit Gateway peering between Transit Gateway in each region.
B> Configure VPC peering between multiple VPCs across different regions.
C> Connect multiple VPCs using interface endpoints.
D> Connect multiple VPCs using AWS Managed VPN.

Explanation:
Correct Answer: A

AWS Transit gateway is a highly scalable and available service that uses AWS global network infrastructure. For connecting VPC between different regions, AWS Transit Gateway in each region needs to be a peer with each other. It allows communication between all the VPCs and can be easily managed at scale.

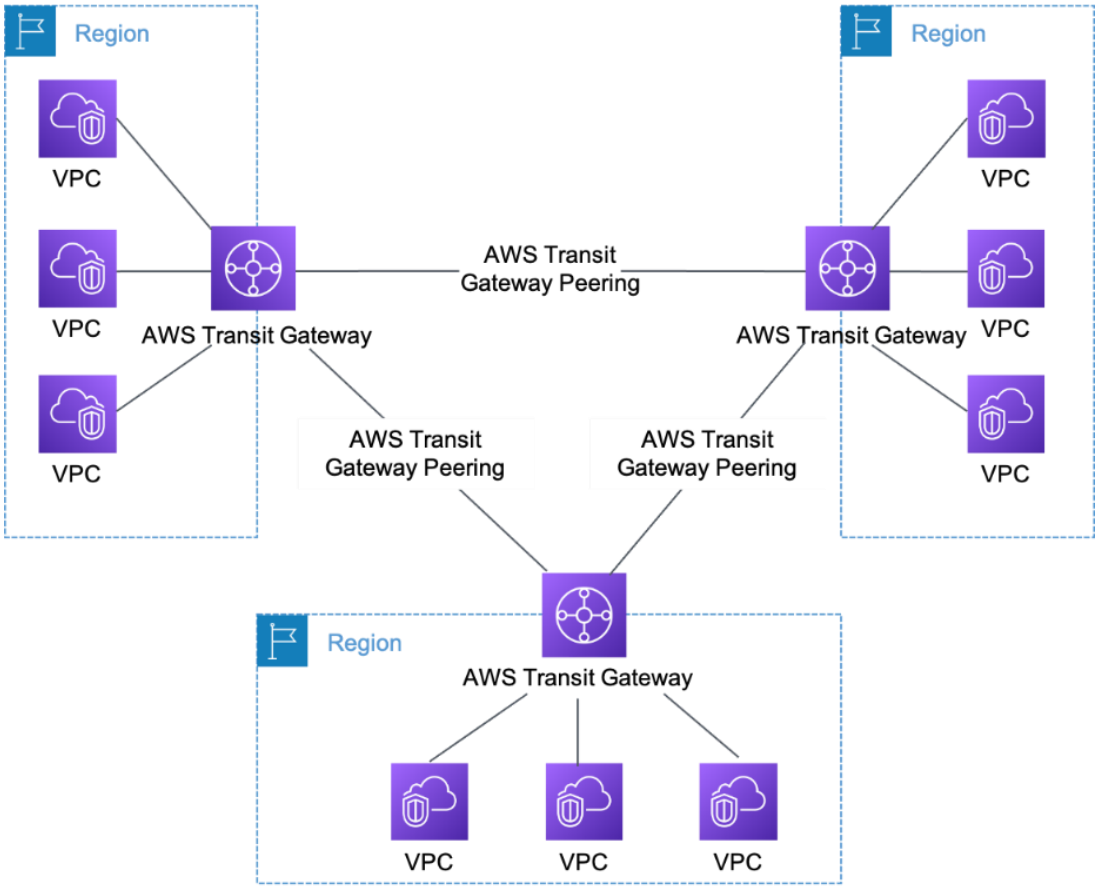


Figure 9 Multi Region multi VPC Peering Connection using Transit Gateway

Option B is incorrect as VPC peering does not support transitive peering, and it would be difficult to manage VPC peering on a scale.
Option C is incorrect as multiple VPCs can be connected using interface endpoints only in a region where these are created.
Option D is incorrect as using managed VPN connections may lead to a sub-optimal routing. Also, redundancy and failover need to be taken care of by the customer.

For reference,

https://docs.aws.amazon.com/whitepapers/latest/aws-vpc-connectivity-options/amazon-vpc-to-amazon-vpc-connectivity-options.html

Question 65 of 65 Domain: Network Security, Compliance, and Governance

84. A company has created multiple accounts as part of an AWS Organization. Each account has multiple VPCs created for deploying applications that are accessed from the Internet Applications are deployed on an Amazon EC2 instance in a private subnet. These instances are front-ended by the Application Load balancer in the public subnet. Internet connectivity is provided by the Internet Gateway attached to each VPC. The Security Team is looking for protecting these applications from bot attacks and exploits such as SQL/XSS attacks. Security solutions should be scalable

and manage application protection for all accounts with least admin work. All the logs captured should be sent in near real-time for further analysis.

What can be deployed to meet these requirements?

A> Deploy AWS WAF on the Amazon EC2 Instance. Use AWS Network Firewall to centrally manage and configure WAF rules for all accounts in an AWS Organization. Enable logging with AWS WAF and send logs to Amazon CloudWatch.

B> Deploy AWS WAF on the Application Load Balancer. Use AWS Network Firewall to centrally manage and configure WAF rules for all accounts in an AWS Organization. Enable logging for AWS WAF and send logs to the Amazon S3 bucket.

C> Deploy AWS WAF on the Amazon EC2 instance. Use AWS Firewall Manager to centrally manage and configure WAF rules for all accounts in an AWS Organization. Enable logging with AWS WAF and send logs to Amazon CloudWatch.

D> Deploy AWS WAF on the Application Load Balancer. Use AWS Firewall Manager to centrally manage and configure WAF rules for all accounts in an AWS Organization. Enable logging for AWS WAF and inject logs to Amazon Kinesis Data Firehose.

Explanation:

Correct Answer: D

AWS WAF can be used for securing web applications from common Layer 7 attacks such as bot attacks and exploits such as SQLI/XSS attacks. AWS WAF can send logs to Amazon CloudWatch, Amazon S3, or Amazon Kinesis Data Firehose. Since, in the above case, logs are required in near real-time for analysis, logs should be sent to Kinesis Data firehose. AWS Firewall Manager is a security management service to centrally manage and configure firewall rules across multiple accounts in an AWS Organization. With the help of AWS Firewall manager, WAF rules can be easily configured on Application Load Balancers across multiple VPCs deployed in multiple accounts.

Option A is incorrect as AWS WAF cannot be deployed directly to the Amazon EC2 instance. AWS Network Firewall can be used for deploying network protection with deep packet inspection at the VPC level. It cannot be used to centrally deploy rules for AWS WAF in multiple accounts. Since near

real-time logs are required for analysis, logs should be sent to Amazon Kinesis Data Firehose and not to Amazon CloudWatch. **Option B is incorrect** as AWS Network Firewall cannot be used to centrally deploy rules for AWS WAF in multiple accounts. Logs are required for analysis and should be sent to Amazon Kinesis Data Firehose, not to the Amazon S3 bucket. **Option C is incorrect** as AWS WAF cannot be deployed directly to Amazon EC2 instances. Logs should be sent to Amazon Kinesis Data Firehose and not to Amazon CloudWatch.

For more information on securing web applications across multiple accounts, refer to the following URL

https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/centralized-inbound-inspection.html