ANS-C01 Q&As

AWS Certified Advanced Networking Specialty Exam

Pass Amazon ANS-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/ans-c01.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A company has a global network and is using transit gateways to connect AWS Regions together. The company finds that two Amazon EC2instances in different Regions are unable to communicate with each other. A network engineer needs to troubleshoot this connectivity issue.What should the network engineer do to meet this requirement?

A. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables and in the VPC route tables. Use VPCflow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

B. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables arecorrect. Use AWS Firewall Manager to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

C. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables arecorrect. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

D. Use VPC Reachability Analyzer to analyze routes in the transit gateway route tables. Verify that the VPC route tables are correct. UseVPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

Correct Answer: C

Network analyzer with VPV flow logs

QUESTION 2

A company is using an AWS Site-to-Site VPN connection from the company\\'s on-premises data center to a virtual private gateway in the AWSCloud Because of congestion, the company is experiencing availability and performance issues as traffic travels across the internet before thetraffic reaches AWS. A network engineer must reduce these issues for the connection as quickly as possible with minimum administrationeffort.Which solution will meet these requirements?

A. Edit the existing Site-to-Site VPN connection by enabling acceleration. Stop and start the VPN service on the customer gateway for thenew setting to take effect.

B. Configure a transit gateway in the same AWS Region as the existing virtual private gateway. Create a new accelerated Site-to-Site VPNconnection. Connect the new connection to the transit gateway by using a VPN attachment. Update the customer gateway device to usethe new Site to Site VPN connection. Delete the existing Site-to-Site VPN connection

C. Create a new accelerated Site-to-Site VPN connection. Connect the new Site-to-Site VPN connection to the existing virtual privategateway. Update the customer gateway device to use the new Site-to-Site VPN connection. Delete the existing Site-to-Site VPNconnection.

D. Create a new AWS Direct Connect connection with a private VIF between the on-premises data center and the AWS Cloud. Update thecustomer gateway device to use the new Direct Connect connection. Delete the existing Site-to-Site VPN connection.

Correct Answer: B

Acceleration is only supported for Site-to-Site VPN connections that are attached to a transit gateway. Virtual private

gateways do not support accelerated VPN connections. https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html

QUESTION 3

A company is in the early stage of AWS Cloud adoption. The company has an application that is running in an on-premises data center in Asia.The company needs to deploy new applications in the us-east-1 Region. The applications in the cloud need connectivity to the on-premisesdata center.The company needs to set up a communication channel between AWS and the data center. The solution must improve latency, minimize thepossibility of performance impact from transcontinental routing over the public internet, and encrypt data in transit.Which solution will meet these requirements in the LEAST amount of time?

A. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a virtual private gateway. Attach the Site-to-Site VPNconnection to the virtual private gateway. Attach the virtual private gateway to the VPC where the applications will be deployed.

B. Create an AWS Site-to-Site VPN connection with acceleration turned on. Create a transit gateway. Attach the Site-to-Site VPNconnection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed.

C. Create an AWS Direct Connect connection. Create a virtual private gateway. Create a public VIF and a private VIF that use the virtualprivate gateway. Create an AWS Site-to-Site VPN connection over the public VIF.

D. Create an AWS Site-to-Site VPN connection with acceleration turned off. Create a transit gateway. Attach the Site-to-Site VPNconnection to the transit gateway. Create a transit gateway attachment to the VPC where the applications will be deployed.

Correct Answer: B

Site to Site VPN with acceleration re-routes your data to AWS Global Acceleration endpoints first, then packets travel on AWS wires to its AWS destination, thus it\\'s faster than traditional VPN connection via direct-connect.

QUESTION 4

A global company runs business applications in the us-east-1 Region inside a VPC. One of the company\\'s regional offices in London uses avirtual private gateway for an AWS Site-to-Site VPN connection tom the VPC. The company has configured a transit gateway and has set uppeering between the VPC and other VPCs that various departments in the company use.Employees at the London office are experiencing latency issues when they connect to the business applications.What should a network engineer do to reduce this latency?

A. Create a new Site-to-Site VPN connection. Set the transit gateway as the target gateway. Enable acceleration on the new Site-to-SiteVPN connection. Update the VPN device in the London office with the new connection details.

B. Modify the existing Site-to-Site VPN connection by setting the transit gateway as the target gateway. Enable acceleration on theexisting Site-to-Site VPN connection.

C. Create a new transit gateway in the eu-west-2 (London) Region. Peer the new transit gateway with the existing transit gateway. Modifythe existing Site-to-Site VPN connection by setting the new transit gateway as the target gateway.

D. Create a new AWS Global Accelerator standard accelerator that has an endpoint of the Site-to-Site VPN connection. Update the VPNdevice in the London office with the new connection details.

Correct Answer: A

https://docs.aws.amazon.com/vpn/latest/s2svpn/accelerated-vpn.html

QUESTION 5

A company hosts a web application that runs on a fleet of Amazon EC2 instances behind an Application Load Balancer (ALB). The instancesare in an Auto Scaling group. The company uses an Amazon CloudFront distribution with the ALB as an origin.The application recently experienced an attack. In response, the company associated an AWS WAF web ACL with the CloudFront distribution.The company needs to use Amazon Athena to analyze application attacks that AWS WAF detects.Which solution will meet this requirement?

A. Configure the ALB and the EC2 instance subnets to produce VPC flow logs. Configure the VPC flow logs to deliver logs to an Amazon S3bucket for log analysis.

B. Create a trail in AWS CloudTrail to capture data events. Configure the trail to deliver logs to an Amazon S3 bucket for log analysis.

C. Configure the AWS WAF web ACL to deliver logs to an Amazon Kinesis Data Firehose delivery stream. Configure the stream to deliverthe data to an Amazon S3 bucket for log analysis.

D. Turn on access logging for the ALB. Configure the access logs to deliver the logs to an Amazon S3 bucket for log analysis.

Correct Answer: C

To send logs to Amazon Kinesis Data Firehose, you send logs from your web ACL to an Amazon Kinesis Data Firehose with a configured storage destination. After you enable logging, AWS WAF delivers logs to your storage destination through the HTTPS endpoint of Kinesis Data Firehose.

QUESTION 6

A company has hundreds of Amazon EC2 instances that are running in two production VPCs across all Availability Zones in the us-east-1Region. The production VPCs are namedVPC A and VPC B.A new security regulation requires all traffic between production VPCs to be inspected before the traffic is routed to its final destination. Thecompany deploys a new shared VPC that contains a stateful firewall appliance and a transit gateway with a VPC attachment across all VPCsto route traffic between VPC A and VPC B through the firewall appliance for inspection. During testing, the company notices that the transitgateway is dropping the traffic whenever the traffic is between two Availability Zones.What should a network engineer do to fix this issue with the LEAST management overhead?

A. In the shared VPC, replace the VPC attachment with a VPN attachment. Create a VPN tunnel between the transit gateway and thefirewall appliance. Configure BGP.

B. Enable transit gateway appliance mode on the VPC attachment in VPC A and VPC B.

C. Enable transit gateway appliance mode on the VPC attachment in the shared VPC.

D. In the shared VPC, configure one VPC peering connection to VPC A and another VPC peering connection to VPC B.

Correct Answer: C

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

the appliance mode must be enabled to keep the traffic in the same firewall appliance, regardless of the AZ where are the source and destination.

When appliance mode is not enabled, a transit gateway attempts to keep traffic routed between VPC attachments in the originating Availability Zone until it reaches its destination.

QUESTION 7

A company is migrating its containerized application to AWS. For the architecture the company will have an ingress VPC with a Network LoadBalancer (NLB) to distribute the traffic to front-end pods in an Amazon Elastic Kubernetes Service (Amazon EKS) cluster. The front end of theapplication will determine which user is requesting access and will send traffic to 1 of 10 services VPCs. Each services VPC will include anNLB that distributes traffic to the services pods in an EKS cluster.The company is concerned about overall cost. User traffic will be responsible for more than 10 TB of data transfer from the ingress VPC toservices VPCs every month. A network engineer needs to recommend how to design the communication between the VPCs.Which solution will meet these requirements at the LOWEST cost?

A. Create a transit gateway. Peer each VPC to the transit gateway. Use zonal DNS names for the NLB in the services VPCs to minimizecross-AZ traffic from the ingress VPC to the services VPCs.

B. Create an AWS PrivateLink endpoint in every Availability Zone in the ingress VPC. Each PrivateLink endpoint will point to the zonal DNSentry of the NLB in the services VPCs.

C. Create a VPC peering connection between the ingress VPC and each of the 10 services VPCs. Use zonal DNS names for the NLB in theservices VPCs to minimize cross-AZ traffic from the ingress VPC to the services VPCs.

D. Create a transit gateway. Peer each VPC to the transit gateway. Turn off cross-AZ load balancing on the transit gateway. Use RegionalDNS names for the NLB in the services VPCs.

Correct Answer: C

VPC peering offers the lowest overall cost when compared to other options for inter-VPC connectivity. https://docs.aws.amazon.com/whitepapers/latest/building-scalable-secure-multi-vpc-network-infrastructure/vpc-to-vpc-connectivity.html

There is no such thing as "TG peering"; there are VPC peering and TG attachments.

QUESTION 8

A company has developed a new web application on AWS. The application runs on Amazon Elastic Container Service (Amazon ECS) on AWSFargate behind an Application Load Balancer (ALB) in the us-east-1 Region. The application uses Amazon Route 53 to host the DNS recordsfor the domain. The content that is served from the website is mostly static images and files that are not updated frequently. Most of thetraffic to the website from end users will originate from the United States. Some traffic will originate from Canada and Europe.A network engineer needs to design a solution that will reduce latency for end users at the lowest cost. The solution also must ensure that alltraffic is encrypted in transit until the traffic reaches the ALB.Which solution will meet these requirements?

A. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create an alias record inAmazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that is assigned to the accelerator forthe ALB.

B. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point tothe DNS record that is assigned to the ALConfigure the CloudFront distribution to use an SSL certificate. Set all behaviors to force HTTPS.Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the DNS name that isassigned to the ALB.

C. Configure the ALB to use a secure HTTPS listener. Create an Amazon CloudFront distribution. Set the origin domain name to point tothe DNS record that is assigned to the ALB. Configure the CloudFront distribution to use an SSL certificate and redirect HTTP to HTTPS.Create an alias record in Amazon Route 53 for the custom domain name. Configure the alias record to route to the CloudFront distribution.

D. Configure the ALB to use an AWS Global Accelerator accelerator in us-east-1. Create a secure HTTPS listener. Create a secondapplication stack on Amazon ECS on Fargate in the eu-west-1 Region. Create another secure HTTPS listener. Create an alias record inAmazon Route 53 for the custom domain name. Configure the alias record to use a latency-based routing policy to route to the DNS namethat is assigned to the accelerator for the ALBs.

Correct Answer: C

Route 53 record points to Cloudfront default DNS name.

QUESTION 9

A network engineer needs to provide dual-stack connectivity between a company\\'s office location and an AWS account. The company\\'s on-premises router supports dual-stack connectivity, and the VPC has been configured with dual-stack support. The company has set up two AWSDirect Connect connections to the office location. This connectivity must be highly available and must be reliable for latency-sensitive traffic.Which solutions will meet these requirements? (Choose two.)

A. Configure a single private VIF on each Direct Connect connection. Add both IPv4 and IPv6 peering to each private VIF. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4 peering and IPv6 routes on the IPv6peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

B. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4peering and IPv6 routes on the IPv6 peering. Enable Bidirectional Forwarding Detection (BFD) on all peering sessions.

C. Configure a single private VIF and IPv4 peering on each Direct Connect connection. Configure the on-premises equipment with thispeering to advertise the IPv6 routes in the same BGP neighbor configuration. Enable Bidirectional Forwarding Detection (BFD) on allpeering sessions.

D. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise all IPv4 routes and IPv6routes on all peering sessions. Keep the Bidirectional Forwarding Detection (BFD) configuration unchanged.

E. Configure two private VIFs on each Direct Connect connection: one private VIF with the IPv4 address family and one private VIF with theIPv6 address family. Configure the on-premises equipment with the AWS provided BGP neighbors to advertise IPv4 routes on the IPv4peering and IPv6 routes on the IPv6 peering. Reduce the BGP hello timer to 5 seconds on both the on-premises equipment and the DirectConnect configuration.

Correct Answer: AB

Both ipv4 and ipv6 BGP sessions can be established with one private VIF

After creating an ipv4 BGP peering on the VIF at the beginning, you can add an ipv6 peering with "add peering" And you have to enable BFD

QUESTION 10

A company deploys a software solution on Amazon EC2 instances that are in a cluster placement group. The solution\\'s UI is a single HTMLpage. The HTML file size is 1,024 bytes. The software processes files that exceed 1,024 MB in size. The software shares files over the networkto clients upon request. The files are shared with the Don\\'t Fragment flag set. Elastic network interfaces of the EC2 instances are set up withjumbo frames.The UI is always accessible from all allowed source IP addresses, regardless of whether the source IP addresses are within a VPC, on theinternet, or on premises. However, clients sometimes do not receive files that they request because the files fail to travel successfully fromthe software to the clients.Which options provide a possible root cause of these failures? (Choose two.)

A. The source IP addresses are from on-premises hosts that are routed over AWS Direct Connect.

B. The source IP addresses are from on-premises hosts that are routed over AWS Site-to-Site VPN.

C. The source IP addresses are from hosts that connect over the public internet.

D. The security group of the EC2 instances does not allow ICMP traffic.

E. The operating system of the EC2 instances does not support jumbo frames.

Correct Answer: BC

Jumbo frames allow more than 1500 bytes of data by increasing the payload size per packet, and thus increasing the percentage of the packet that is not packet overhead. Fewer packets are needed to send the same amount of usable data. However, traffic is limited to a maximum MTU of 1500 in the following cases:

Traffic over an internet gateway

Traffic over an inter-region VPC peering connection

Traffic over VPN connections

Traffic outside of a given AWS Region for EC2-Classic

If packets are over 1500 bytes, they are fragmented, or they are dropped if the Don\\'t Fragment flag is set in the IP header.

regardless the security group allows icmp traffic to enable pmtud or not, the oversized packets will be dropped anyway due to don\\'t fragment flag set.

QUESTION 11

A company is hosting an application on Amazon EC2 instances behind an Application Load Balancer. The instances are in an Amazon EC2Auto Scaling group. Because of a recent change to a security group, external users cannot access the application.A network engineer needs to prevent this downtime from happening again. The network engineer must implement a solution that remediatesnoncompliant changes to security groups.Which solution will meet these requirements?

A. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

B. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

C. Configure Amazon GuardDuty to detect inconsistencies between the desired security group configuration and the

current security groupconfiguration. Configure AWS OpsWorks for Chef to remediate noncompliant security groups.

D. Configure an AWS Config rule to detect inconsistencies between the desired security group configuration and the current security groupconfiguration. Create an AWS Systems Manager Automation runbook to remediate noncompliant security groups.

Correct Answer: D

https://aws.amazon.com/blogs/mt/remediate-noncompliant-aws-config-rules-with-aws-systems-manager-automation-runbooks/

QUESTION 12

A company hosts its IT infrastructure in an on-premises data center. The company wants to migrate the infrastructure to the AWS Cloud inphases. A network engineer wants to set up a 10 Gbps AWS Direct Connect dedicated connection between the on-premises data center andVPCs. The company\\'s network provider needs 3 months to provision the Direct Connect connection.In the meantime, the network engineer implements a temporary solution by deploying an AWS Siteto-Site VPN connection that terminates toa virtual private gateway. The network engineer observes that the bandwidth of the Site-to-Site VPN connection is capped at 1.25 Gbpsdespite a powerful customer gateway device.What should the network engineer do to improve the VPN connection bandwidth before the implementation of the Direct Connect connection?

A. Contact AWS Support to request a bandwidth quota increase for the existing Site-to-Site VPN connection.

B. Discuss the issue with the hardware vendor. Buy a bigger and more powerful customer gateway device that has faster encryption anddecryption capabilities.

C. Create several additional Site-to-Site VPN connections that terminate on the same virtual gateway. Configure equal-cost multi-path(ECMP) routing to use all the VPN connections simultaneously.

D. Create a transit gateway. Attach the VPCs to the transit gateway. Create several additional Site-to-Site VPN connections that terminateon the transit gateway. Configure equal-cost multi-path (ECMP) routing to use all the VPN connections simultaneously.

Correct Answer: D

ECMP is not supported for Site-to-Site VPN connections on a virtual private gateway.

You can check this document: https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html

QUESTION 13

A financial company that is located in the us-east-1 Region needs to establish secure connectivity to AWS. The company has two on-premisesdata centers, each located within the same Region. The company\\'s network team needs to establish hybrid connectivity to its AWSenvironment with reliable and consistent connectivity.The connection must provide access to the company\\'s private resources inside its AWS environment. The resources are located in the us-east-1 and us-west-2 Regions. The connection must allow resources from the corporate networks to send large amounts of data to Amazon S3 overthe same connection. To meet compliance requirements, the connection must be highly available and must provide encryption for all packetsthat are sent between the on-premises location and any services on AWS.Which combination of steps should the network team take to meet these requirements? (Choose two.)

A. Set up a private VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the private VIF to

encrypt data in transitto the VPCs in us-east-1 and us-west-2.

B. Set up an AWS Direct Connect connection to each of the company\\'s data centers.

C. Set up an AWS Direct Connect connection from one of the company\\'s data centers to us-east-1 and us-west-2.

D. Set up a public VIF to send data to Amazon S3. Use an AWS Site-to-Site VPN connection over the public VIF to encrypt data in transit tothe VPCs in us-east-1 and us-west-2.

E. Set up a transit VIF for an AWS Direct Connect gateway to send data to Amazon S3. Create a transit gateway. Associate the transitgateway with the Direct Connect gateway to provide secure communications from the company\\'s data centers to the VPCs in us-east-1 andus-west-2.

Correct Answer: BD

Option B: Establishing an AWS Direct Connect connection to each of the company\\'s data centers ensures a reliable, consistent connection. This setup also addresses the requirement for high availability. If there are problems with one connection, the other connection can maintain the data flow.

Option D: A public VIF can provide direct access to AWS services, including Amazon S3, across the Direct Connect link. By using an AWS Site-to-Site VPN connection over the public VIF, you can encrypt data in transit between the on-premises location and the VPCs in us-east-1 and us-west-2, thereby meeting the company\\'s compliance requirements.

QUESTION 14

A company has business operations in the United States and in Europe. The company\\'s public applications are running on AWS and use threetransit gateways. The transit gateways are located in the us-west-2, us-east-1, and eu-central-1 Regions. All the transit gateways areconnected to each other in a full mesh configuration.The company accidentally removes the route to the eu-central-1 VPCs from the us-west-2 transit gateway route table. The company alsoaccidentally removes the route to the us-west-2 VPCs from the eu-central-1 transit gateway route table.How can a network engineer identify the misconfiguration with the LEAST operational overhead?

A. Use the Route Analyzer feature for AWS Transit Gateway Network Manager.

B. Use the AWSSupport-SetupIPMonitoringFromVPC AWS Systems Manager Automation runbook. Push network telemetry data to AmazonCloudWatch Logs for analysis.

C. Use VPC flow logs in eu-central-1 and us-west-2 to analyze the missing routes.

D. Use Amazon VPC Traffic Mirroring in eu-central-1 or us-west-2 to take packet captures and troubleshoot the connectivity issues.

Correct Answer: A

https://docs.aws.amazon.com/network-manager/latest/tgwnm/route-analyzer.html

QUESTION 15

A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Regiononly. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an AutoScaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. TheALB is in a public subnet and allows

inbound traffic only from partner network IP address ranges over port 80.When the company adds a new partner, the company must allow the IP address range of the partner network in the security group that isassociated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP addressranges.Which solution will meet these requirements in the MOST operationally efficient manner?

A. Create an Amazon DynamoDB table to maintain all IP address ranges and security groups that need to be updated. Update theDynamoDB table with the new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IPaddress ranges and security groups from the DynamoDB table to update the security groups. Deploy this solution in all accounts.

B. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Use Amazon EventBridge (Amazon CloudWatch Events)rules to invoke an AWS Lambda function to update security groups whenever a new IP address range is added to the prefix list. Deploy thissolution in all accounts.

C. Create a new prefix list. Add all allowed IP address ranges to the prefix list. Share the prefix list across different accounts by using AWSResource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address range. Update theprefix list with the new IP address range when the company adds a new partner.

D. Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be updated. Update the S3 bucket withthe new IP address range when the company adds a new partner. Invoke an AWS Lambda function to read new IP address ranges andsecurity groups from the S3 bucket to update the security groups. Deploy this solution in all accounts.

Correct Answer: C

ttps://docs.aws.amazon.com/vpc/latest/userguide/managed-prefix-lists.html