Amazon-Web-Services

Exam Questions ANS-C01

AWS Certified Advanced Networking Specialty Exam

NEW QUESTION 1
An IoT company sells hardware sensor modules that periodically send out temperature, humidity, pressure, and location data through the MQTT messaging protocol. The hardware sensor modules send this data to the company's on-premises MQTT brokers that run on Linux servers behind a load balancer. The hardware sensor modules have been hardcoded with public IP addresses to reach the brokers.
The company is growing and is acquiring customers across the world. The existing solution can no longer scale and is introducing additional latency because of the company's global presence. As a result, the company decides to migrate its entire infrastructure from on premises to the AWS Cloud. The company needs to migrate without reconfiguring the hardware sensor modules that are already deployed across the world. The solution also must minimize latency.
The company migrates the MQTT brokers to run on Amazon EC2 instances. What should the company do next to meet these requirements?

A. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listener
B. Use Bring Your Own IP (BYOIP) from the on-premises network with the NLB.
C. Place the EC2 instances behind a Network Load Balancer (NLB). Configure TCP listener
D. Create an AWS Global Accelerator accelerator in front of the NLUse Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator.
E. Place the EC2 instances behind an Application Load Balancer (ALB). Configure TCP listener
F. Create an AWS Global Accelerator accelerator in front of the AL
G. Use Bring Your Own IP (BYOIP) from the on-premises network with Global Accelerator
H. Place the EC2 instances behind an Amazon CloudFront distributio
I. Use Bring Your Own IP (BYOIP) from the on-premises network with CloudFront.

Answer: B

NEW QUESTION 2
A network engineer must develop an AWS CloudFormation template that can create a virtual private gateway, a customer gateway, a VPN connection, and static routes in a route table. During testing of the template, the network engineer notes that the CloudFormation template has encountered an error and is rolling back.
What should the network engineer do to resolve the error?

A. Change the order of resource creation in the CloudFormation template.
B. Add the DependsOn attribute to the resource declaration for the virtual private gatewa
C. Specify the route table entry resource.
D. Add a wait condition in the template to wait for the creation of the virtual private gateway.
E. Add the DependsOn attribute to the resource declaration for the route table entr
F. Specify the virtual private gateway resource.

Answer: D

NEW QUESTION 3
A data analytics company has a 100-node high performance computing (HPC) cluster. The HPC cluster is for parallel data processing and is hosted in a VPC in the AWS Cloud. As part of the data processing workflow, the HPC cluster needs to perform several DNS queries to resolve and connect to Amazon RDS databases, Amazon S3 buckets, and on-premises data stores that are accessible through AWS Direct Connect. The HPC cluster can increase in size by five to seven times during the company's peak event at the end of the year.
The company is using two Amazon EC2 instances as primary DNS servers for the VPC. The EC2 instances are configured to forward queries to the default VPC resolver for Amazon Route 53 hosted domains and to the on-premises DNS servers for other on-premises hosted domain names. The company notices job failures and finds that DNS queries from the HPC cluster nodes failed when the nodes tried to resolve RDS and S3 bucket endpoints.
Which architectural change should a network engineer implement to provide the DNS service in the MOST scalable way?

A. Scale out the DNS service by adding two additional EC2 instances in the VP
B. Reconfigure half of the HPC cluster nodes to use these new DNS server
C. Plan to scale out by adding additional EC2instance-based DNS servers in the future as the HPC cluster size grows.
D. Scale up the existing EC2 instances that the company is using as DNS server
E. Change the instance size to the largest possible instance size to accommodate the current DNS load and theanticipated load in the future.
F. Create Route 53 Resolver outbound endpoint
G. Create Route 53 Resolver rules to forward queries to on-premises DNS servers for on premises hosted domain name
H. Reconfigure the HPC cluster nodes to use the default VPC resolver instead of the EC2 instance-based DNS server
I. Terminate the EC2 instances.
J. Create Route 53 Resolver inbound endpoint
K. Create rules on the on-premises DNS servers to forward queries to the default VPC resolve
L. Reconfigure the HPC cluster nodes to forward all DNS queries to the on-premises DNS server
M. Terminate the EC2 instances.

Answer: C

NEW QUESTION 4
A company has its production VPC (VPC-A) in the eu-west-1 Region in Account 1. VPC-A is attached to a transit gateway (TGW-A) that is connected to an on-premises data center in Dublin, Ireland, by an AWS
Direct Connect transit VIF that is configured for an AWS Direct Connect gateway. The company also has a staging VPC (VPC-B) that is attached to another transit gateway (TGW-B) in the eu-west-2 Region in Account 2.
A network engineer must implement connectivity between VPC-B and the on-premises data center in Dublin. Which solutions will meet these requirements? (Choose two.)

A. Configure inter-Region VPC peering between VPC-A and VPC-
B. Add the required VPC peering route
C. Add the VPC-B CIDR block in the allowed prefixes on the Direct Connect gateway association.
D. Associate TGW-B with the Direct Connect gatewa
E. Advertise the VPC-B CIDR block under the allowed prefixes.
F. Configure another transit VIF on the Direct Connect connection and associate TGW-
G. Advertise the VPC-B CIDR block under the allowed prefixes.
H. Configure inter-Region transit gateway peering between TGW-A and TGW-
I. Add the peering routes in the transit gateway route table

J. Add both the VPC-A and the VPC-B CIDR block under the allowed prefix list in the Direct Connect gateway association.
K. Configure an AWS Site-to-Site VPN connection over the transit VIF to TGW-B as a VPN attachment.

Answer: BC

Explanation:
* B. Associate TGW-B with the Direct Connect gateway. Advertise the VPC-B CIDR block under the allowed prefixes. This will allow traffic from VPC-B to be sent over the Direct Connect connection to the on-premises data center via TGW-B. C. Configure another transit VIF on the Direct Connect connection and associate TGW-B. Advertise the VPC-B CIDR block under the allowed prefixes. This will enable the use of the Direct Connect connection for VPC-B's traffic by connecting TGW-B to the Direct Connect gateway.

NEW QUESTION 5
A company has deployed a web application on AWS. The web application uses an Application Load Balancer (ALB) across multiple Availability Zones. The targets of the ALB are AWS Lambda functions. The web application also uses Amazon CloudWatch metrics for monitoring.
Users report that parts of the web application are not loading properly. A network engineer needs to troubleshoot the problem. The network engineer enables access logging for the ALB.
What should the network engineer do next to determine which errors the ALB is receiving?

A. Send the logs to Amazon CloudWatch Log
B. Review the ALB logs in CloudWatch Insights to determine which error messages the ALB is receiving.
C. Configure the Amazon S3 bucket destinatio
D. Use Amazon Athena to determine which error messages the ALB is receiving.
E. Configure the Amazon S3 bucket destinatio
F. After Amazon CloudWatch Logs pulls the ALB logs from the S3 bucket automatically, review the logs in CloudWatch Logs to determine which error messages the ALB is receiving.
G. Send the logs to Amazon CloudWatch Log
H. Use the Amazon Athena CloudWatch Connector todetermine which error messages the ALB is receiving.

Answer: B

Explanation:
Access logs is an optional feature of Elastic Load Balancing that is disabled by default. After you enable access logs for your load balancer, Elastic Load Balancing captures the logs and stores them in the Amazon S3 bucket that you specify as compressed files. You can disable access logs at any time.https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-access-logs.html

NEW QUESTION 6
A company has hundreds of VPCs on AWS. All the VPCs access the public endpoints of Amazon S3 and AWS Systems Manager through NAT gateways. All the traffic from the VPCs to Amazon S3 and Systems Manager travels through the NAT gateways. The company's network engineer must centralize access to these services and must eliminate the need to use public endpoints.
Which solution will meet these requirements with the LEAST operational overhead?

A. Create a central egress VPC that has private NAT gateway
B. Connect all the VPCs to the central egress VPC by using AWS Transit Gatewa
C. Use the private NAT gateways to connect to Amazon S3 and Systems Manager by using private IP addresses.
D. Create a central shared services VP
E. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
F. Ensure that private DNS is turned of
G. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
H. Create an Amazon Route 53 forwarding rule for each interface VPC endpoin
I. Associate the forwarding rules with all the VPC
J. Forward DNS queries to the interface VPC endpoints in the shared services VPC.
K. Create a central shared services VPIn the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
L. Ensure that private DNS is turned of
M. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
N. Create an Amazon Route 53 private hosted zone with a full service endpoint name for Amazon S3 and Systems Manage
O. Associate the private hosted zones with all the VPC
P. Create an alias record in each private hosted zone with the full AWS service endpoint pointing to the interface VPC endpoint in the shared services VPC.
Q. Create a central shared services VP
R. In the central shared services VPC, create interface VPC endpoints for Amazon S3 and Systems Manager to acces
S. Connect all the VPCs to the central shared services VPC by using AWS Transit Gatewa
T. Ensure that private DNS is turned on for the interface VPC endpoints and that the transit gateway is created with DNS support turned on.

Answer: B

Explanation:
Interface VPC endpoints enable private connectivity between VPCs and supported AWS serviceswithout requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection2. Interface VPC endpoints are powered by AWS PrivateLink, a technology that enables private access to AWS services2. Amazon S3 and AWS Systems Manager support interface VPC endpoin2ts. By turning off private DNS, the interface VPC endpoints can be accessed by using their private IP addresses2. By using Amazon Route 53 forwarding rules, DNS queries can be resolved to the interface VPC endpoints in the shared services VPC3.

NEW QUESTION 7
A real estate company is building an internal application so that real estate agents can upload photos and videos of various properties. The application will store these photos and videos in an Amazon S3 bucket as objects and will use Amazon DynamoDB to store corresponding metadata. The S3 bucket will be configured to publish all PUT events for new object uploads to an Amazon Simple Queue Service (Amazon SQS) queue.
A compute cluster of Amazon EC2 instances will poll the SQS queue to find out about newly uploaded objects. The cluster will retrieve new objects, perform proprietary image and video recognition and classification update metadata in DynamoDB and replace the objects with new watermarked objects. The company does not want public IP addresses on the EC2 instances.
Which networking design solution will meet these requirements MOST cost-effectively as application usage increases?

A. Place the EC2 instances in a public subne
B. Disable the Auto-assign Public IP option while launching the EC2 instance
C. Create an internet gatewa
D. Attach the internet gateway to the VP
E. In the public subnet's route table, add a default route that points to the internet gateway.
F. Place the EC2 instances in a private subne
G. Create a NAT gateway in a public subnet in the same Availability Zon
H. Create an internet gatewa
I. Attach the internet gateway to the VP
J. In the public subnet's route table, add a default route that points to the internet gateway
K. Place the EC2 instances in a private subne
L. Create an interface VPC endpoint for Amazon SQ
M. Create gateway VPC endpoints for Amazon S3 and DynamoDB.
N. Place the EC2 instances in a private subne
O. Create a gateway VPC endpoint for Amazon SQS.Create interface VPC endpoints for Amazon S3 and DynamoDB.

Answer: C

NEW QUESTION 8
All IP addresses within a 10.0.0.0/16 VPC are fully utilized with application servers across two Availability Zones. The application servers need to send frequent UDP probes to a single central authentication server on the Internet to confirm that is running up-to-date packages. The network is designed for application servers to use a single NAT gateway for internal access. Testing reveals that a few of the servers are unable to communicate with the authentication server.

A. The NAT gateway does not support UDP traffic.
B. The authentication server is not accepting traffic.
C. The NAT gateway cannot allocate more ports.
D. The NAT gateway is launched in a private subnet.

Answer: C

Explanation:
Ref:https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
"A NAT gateway can support up to 55,000 simultaneous connections to each unique destination. This limit also applies if you create approximately 900 connections per second to a single destination (about 55,000 connections per minute). If the destination IP address, the destination port, or the protocol (TCP/UDP/ICMP) changes, you can create an additional 55,000 connections. For more than 55,000 connections, there is an increased chance of connection errors due to port allocation errors. These errors can be monitored by viewing the ErrorPortAllocation CloudWatch metric for your NAT gateway. For more information, see Monitoring NAT Gateways Using Amazon CloudWatch."

NEW QUESTION 9
A company's network engineer is designing a hybrid DNS solution for an AWS Cloud workload. Individual teams want to manage their own DNS hostnames for their applications in their development environment. The solution must integrate the application-specific hostnames with the centrally managed DNS hostnames from the on-premises network and must provide bidirectional name resolution. The solution also must minimize management overhead.
Which combination of steps should the network engineer take to meet these requirements? (Choose three.)

A. Use an Amazon Route 53 Resolver inbound endpoint.
B. Modify the DHCP options set by setting a custom DNS server value.
C. Use an Amazon Route 53 Resolver outbound endpoint.
D. Create DNS proxy servers.
E. Create Amazon Route 53 private hosted zones.
F. Set up a zone transfer between Amazon Route 53 and the on-premises DNS.

Answer: ABE

NEW QUESTION 10
A network engineer needs to set up an Amazon EC2 Auto Scaling group to run a Linux-based network appliance in a highly available architecture. The network engineer is configuring the new launch template for the Auto Scaling group.
In addition to the primary network interface the network appliance requires a second network interface that will be used exclusively by the application to exchange traffic with hosts over the internet. The company has set up a Bring Your Own IP (BYOIP) pool that includes an Elastic IP address that should be used as the public IP address for the second network interface.
How can the network engineer implement the required architecture?

A. Configure the two network interfaces in the launch templat
B. Define the primary network interface to be created in one of the private subnet
C. For the second network interface, select one of the public subnet
D. Choose the BYOIP pool ID as the source of public IP addresses.
E. Configure the primary network interface in a private subnet in the launch templat
F. Use the user data option to run a cloud-init script after boot to attach the second network interface from a subnet with auto-assign public IP addressing enabled.
G. Create an AWS Lambda function to run as a lifecycle hook of the Auto Scaling group when an instance is launchin
H. In the Lambda function, assign a network interface to an AWS Global Accelerator endpoint.
I. During creation of the Auto Scaling group, select subnets for the primary network interfac
J. Use the user data option to run a cloud-init script to allocate a second network interface and to associate anElastic IP address from the BYOIP pool.

Answer: D

Explanation:
During creation of the Auto Scaling group, select subnets for the primary network interface. Use the user data option to run a cloud-init script to allocate a second network interface and to associate an Elastic IP address from the BYOIP pool.
This solution meets all of the requirements stated in the question. The primary network interface can be configured in a private subnet during creation of the Auto Scaling group. The user data option can be used to run a cloud-init script that will allocate a second network interface and associate an Elastic IP address from the BYOIP pool with it.

NEW QUESTION 10
Your organization has a newly installed 1-Gbps AWS Direct Connect connection. You order the cross-connect from the Direct Connect location provider to the port on your router in the same facility. To enable the use of your first virtual interface, your router must be configured appropriately.
What are the minimum requirements for your router?

A. 1-Gbps Multi Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
B. 1-Gbps Single Mode Fiber Interface, 802.1Q VLAN, Peer IP Address, BGP Session with MD5.
C. IPsec Parameters, Pre-Shared key, Peer IP Address, BGP Session with MD5
D. BGP Session with MD5, 802.1Q VLAN, Route-Map, Prefix List, IPsec encrypted GRE Tunnel

Answer: B

NEW QUESTION 12
You deploy an Amazon EC2 instance that runs a web server into a subnet in a VPC. An Internet gateway is attached, and the main route table has a default route (0.0.0.0/0) configured with a target of the Internet gateway.
The instance has a security group configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

The Network ACL for the subnet is configured to allow as follows:

- Protocol: TCP
- Port: 80 inbound, nothing outbound

When you try to browse to the web server, you receive no response. Which additional step should you take to receive a successful response?

A. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 80
B. Add an entry to the security group outbound rules for Protocol: TCP, Port Range: 1024-65535
C. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 80
D. Add an entry to the Network ACL outbound rules for Protocol: TCP, Port Range: 1024-65535

Answer: D

Explanation:
To enable the connection to a service running on an instance, the associated network ACL must allow both inbound traffic on the port that the service is listening on as well as allow outbound traffic from ephemeral ports. When a client connects to a server, a random port from the ephemeral port range (1024-65535) becomes the client's source port. The designated ephemeral port then becomes the destination port for return traffic from the service, so outbound traffic from the ephemeral port must be allowed in the network ACL.https://aws.amazon.com/premiumsupport/knowledge-center/resolve-connection-sg-acl-inbound/

NEW QUESTION 16
A company uses a 1 Gbps AWS Direct Connect connection to connect its AWS environment to its
on-premises data center. The connection provides employees with access to an application VPC that is hosted on AWS. Many remote employees use a company-provided VPN to connect to the data center. These employees are reporting slowness when they access the application during business hours. On-premises users have started to report similar slowness while they are in the office.
The company plans to build an additional application on AWS. On-site and remote employees will use the additional application. After the deployment of this additional application, the company will need 20% more bandwidth than the company currently uses. With the increased usage, the company wants to add resiliency to the AWS connectivity. A network engineer must review the current implementation and must make improvements within a limited budget.
What should the network engineer do to meet these requirements MOST cost-effectively?

A. Set up a new 1 Gbps Direct Connect dedicated connection to accommodate the additional traffic load from remote employees and the additional applicatio
B. Create a link aggregation group (LAG).
C. Deploy an AWS Site-to-Site VPN connection to the application VP
D. Configure the on-premises routing for the remote employees to connect to the Site-to-Site VPN connection.
E. Deploy Amazon Workspaces into the application VPInstruct the remote employees to connect to Workspaces.
F. Replace the existing 1 Gbps Direct Connect connection with two new 2 Gbps Direct Connect hosted connection
G. Create an AWS Client VPN endpoint in the application VP
H. Instruct the remote employees to connect to the Client VPN endpoint.

Answer: A

Explanation:
Setting up a new 1 Gbps Direct Connect dedicated connection to accommodate the additional trafficload from remote employees and the additional application would provide more bandwidth and lower latency than a VPN connection over the public internet1. Creating a link aggregation group (LAG) with the existing and new Direct Connect connections would provide resiliency and redundancy for the AWS connectivity2.

NEW QUESTION 20
A global delivery company is modernizing its fleet management system. The company has several business units. Each business unit designs and maintains applications that are hosted in its own AWS account in separate application VPCs in the same AWS Region. Each business unit's applications are designed to get data from a central shared services VPC.
The company wants the network connectivity architecture to provide granular security controls. The architecture also must be able to scale as more business units consume data from the central shared services VPC in the future.
Which solution will meet these requirements in the MOST secure manner?

A. Create a central transit gatewa
B. Create a VPC attachment to each application VP
C. Provide full mesh connectivity between all the VPCs by using the transit gateway.
D. Create VPC peering connections between the central shared services VPC and each application VPC in each business unit's AWS account.
E. Create VPC endpoint services powered by AWS PrivateLink in the central shared services VPCreate VPC endpoints in each application VPC.
F. Create a central transit VPC with a VPN appliance from AWS Marketplac
G. Create a VPN attachment from each VPC to the transit VP

H. Provide full mesh connectivity among all the VPCs.

Answer: C

Explanation:
Option C provides a secure and scalable solution using VPC endpoint services powered by AWS PrivateLink. AWS PrivateLink enables private connectivity between VPCs and services without exposing the data to the public internet or using a VPN connection. By creating VPC endpoints in each application VPC, the company can securely access the central shared services VPC without the need for complex network configurations. Furthermore, PrivateLink supports cross-account connectivity, which makes it a scalable solution as more business units consume data from the central shared services VPC in the future.

NEW QUESTION 21
A company has deployed a software-defined WAN (SD-WAN) solution to interconnect all of its offices. The company is migrating workloads to AWS and needs to extend its SD-WAN solution to support connectivity to these workloads.
A network engineer plans to deploy AWS Transit Gateway Connect and two SD-WAN virtual appliances to provide this connectivity. According to company policies, only a single SD-WAN virtual appliance can handle traffic from AWS workloads at a given time.
How should the network engineer configure routing to meet these requirements?

A. Add a static default route in the transit gateway route table to point to the secondary SD-WAN virtual applianc
B. Add routes that are more specific to point to the primary SD-WAN virtual appliance.
C. Configure the BGP community tag 7224:7300 on the primary SD-WAN virtual appliance for BGP routes toward the transit gateway.
D. Configure the AS_PATH prepend attribute on the secondary SD-WAN virtual appliance for BGP routes toward the transit gateway.
E. Disable equal-cost multi-path (ECMP) routing on the transit gateway for Transit Gateway Connect.

Answer: A

NEW QUESTION 22
A company is using Amazon Route 53 Resolver DNS Firewall in a VPC to block all domains except domains that are on an approved list. The company is concerned that if DNS Firewall is unresponsive, resources in the VPC might be affected if the network cannot resolve any DNS queries. To maintain application service level agreements, the company needs DNS queries to continue to resolve even if Route 53 Resolver does not receive a response from DNS Firewall.
Which change should a network engineer implement to meet these requirements?

A. Update the DNS Firewall VPC configuration to disable fail open for the VPC.
B. Update the DNS Firewall VPC configuration to enable fail open for the VPC.
C. Create a new DHCP options set with parameter dns_firewall_fail_open=fals
D. Associate the new DHCP options set with the VPC.
E. Create a new DHCP options set with parameter dns_firewall_fail_open=tru
F. Associate the new DHCP options set with the VPC.

Answer: B

NEW QUESTION 26
A company plans to deploy a two-tier web application to a new VPC in a single AWS Region. The company has configured the VPC with an internet gateway and four subnets. Two of the subnets are public and have default routes that point to the internet gateway. Two of the subnets are private and share a route table that does not have a default route.
The application will run on a set of Amazon EC2 instances that will be deployed behind an external Application Load Balancer. The EC2 instances must not be directly accessible from the internet. The application will use an Amazon S3 bucket in the same Region to store data. The application will invoke S3 GET API operations and S3 PUT API operations from the EC2 instances. A network engineer must design a VPC architecture that minimizes data transfer cost.
Which solution will meet these requirements?

A. Deploy the EC2 instances in the public subnet
B. Create an S3 interface endpoint in the VP
C. Modify the application configuration to use the S3 endpoint-specific DNS hostname.
D. Deploy the EC2 instances in the private subnet
E. Create a NAT gateway in the VP
F. Create default routes in the private subnets to the NAT gatewa
G. Connect to Amazon S3 by using the NAT gateway.
H. Deploy the EC2 instances in the private subnet
I. Create an S3 gateway endpoint in the VPSpecify die route table of the private subnets during endpoint creation to create routes to Amazon S3.
J. Deploy the EC2 instances in the private subnet
K. Create an S3 interface endpoint in the VP
L. Modify the application configuration to use the S3 endpoint-specific DNS hostname.

Answer: C

Explanation:
Option C is the optimal solution as it involves deploying the EC2 instances in the private subnets, which provides additional security benefits. Additionally, creating an S3 gateway endpoint in the VPC will enable the EC2 instances to communicate with Amazon S3 directly, without incurring data transfer costs. This is because the S3 gateway endpoint uses Amazon's private network to transfer data between the VPC and S3, which is not charged for data transfer. Furthermore, specifying the route table of the private subnets during endpoint creation will create routes to Amazon S3, which is required for the EC2 instances to communicate with S3.

NEW QUESTION 28
A company has created three VPCs: a production VPC, a nonproduction VPC, and a shared services VPC. The production VPC and the nonproduction VPC must each have communication with the shared services VPC. There must be no communication between the production VPC and the nonproduction VPC. A transit gateway is deployed to facilitate communication between VPCs.
Which route table configurations on the transit gateway will meet these requirements?

A. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for only the shared services VP
B. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
C. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes for each VP

D. Create an additional route table with only the shared services VPC attachment associated with propagated routes from each VPC.
E. Configure a route table with all the VPC attachments associated with propagated routes for only the shared services VPCCreate an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.
F. Configure a route table with the production and nonproduction VPC attachments associated with propagated routes disable
G. Create an additional route table with only the shared services VPC attachment associated with propagated routes from the production and nonproduction VPCs.

Answer: A

NEW QUESTION 33
A network engineer must provide additional safeguards to protect encrypted data at Application Load Balancers (ALBs) through the use of a unique random session key.
What should the network engineer do to meet this requirement?

A. Change the ALB security policy to a policy that supports TLS 1.2 protocol only
B. Use AWS Key Management Service (AWS KMS) to encrypt session keys
C. Associate an AWS WAF web ACL with the ALB
D. and create a security rule to enforce forward secrecy (FS)
E. Change the ALB security policy to a policy that supports forward secrecy (FS)

Answer: D

NEW QUESTION 34
A company has deployed an AWS Network Firewall firewall into a VPC. A network engineer needs to implement a solution to deliver Network Firewall flow logs to the company's Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster in the shortest possible time.
Which solution will meet these requirements?

A. Create an Amazon S3 bucke
B. Create an AWS Lambda function to load logs into the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluste
C. Enable Amazon Simple Notification Service (Amazon SNS) notifications on the S3 bucket to invoke the Lambda functio
D. Configure flow logs for the firewal
E. Set the S3 bucket as the destination.
F. Create an Amazon Kinesis Data Firehose delivery stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destinatio
G. Configure flow logs for the firewall Set the Kinesis Data Firehose delivery stream as the destination for the Network Firewall flow logs.
H. Configure flow logs for the firewal
I. Set the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destination for the Network Firewall flow logs.
J. Create an Amazon Kinesis data stream that includes the Amazon OpenSearch Service (Amazon Elasticsearch Service) cluster as the destinatio
K. Configure flow logs for the firewal
L. Set the Kinesis data stream as the destination for the Network Firewall flow logs.

Answer: B

Explanation:
https://aws.amazon.com/blogs/networking-and-content-delivery/how-to-analyze-aws-network-firewall-logs-usin

NEW QUESTION 37
A global company operates all its non-production environments out of three AWS Regions: eu-west-1,
us-east-1, and us-west-1. The company hosts all its production workloads in two on-premises data centers. The company has 60 AWS accounts and each account has two VPCs in each Region. Each VPC has a virtual private gateway where two VPN connections terminate for resilient connectivity to the data centers. The company has 360 VPN tunnels to each data center, resulting in high management overhead. The total VPN throughput for each Region is 500 Mbps.
The company wants to migrate the production environments to AWS. The company needs a solution that will simplify the network architecture and allow for future growth. The production environments will generate an additional 2 Gbps of traffic per Region back to the data centers. This traffic will increase over time.
Which solution will meet these requirements?

A. Set up an AWS Direct Connect connection from each data center to AWS in each Regio
B. Create and attach private VIFs to a single Direct Connect gatewa
C. Attach the Direct Connect gateway to all the VPC
D. Remove the existing VPN connections that are attached directly to the virtual private gateways.
E. Create a single transit gateway with VPN connections from each data cente
F. Share the transit gateway with each account by using AWS Resource Access Manager (AWS RAM). Attach the transit gateway to each VP
G. Remove the existing VPN connections that are attached directly to the virtual private gateways.
H. Create a transit gateway in each Region with multiple newly commissioned VPN connections from each data cente
I. Share the transit gateways with each account by using AWS Resource Access Manager (AWS RAM). In each Region, attach the transit gateway to each VPRemove the existing VPN connections that are attached directly to the virtual private gateways.
J. Peer all the VPCs in each Region to a new VPC in each Region that will function as a centralized transit VP
K. Create new VPN connections from each data center to the transit VPC
L. Terminate the original VPN connections that are attached to all the original VPC
M. Retain the new VPN connection to the new transit VPC in each Region.

Answer: C

NEW QUESTION 39
A company has a hybrid cloud environment. The company's data center is connected to the AWS Cloud by an AWS Direct Connect connection. The AWS environment includes VPCs that are connected together in a hub-and-spoke model by a transit gateway. The AWS environment has a transit VIF with a Direct Connect gateway for on-premises connectivity.
The company has a hybrid DNS model. The company has configured Amazon Route 53 Resolver endpoints in the hub VPC to allow bidirectional DNS traffic flow. The company is running a backend application in one of the VPCs.
The company uses a message-oriented architecture and employs Amazon Simple Queue Service (Amazon SQS) to receive messages from other applications over a private network. A network engineer wants to use an interface VPC endpoint for Amazon SQS for this architecture. Client services must be able to access

the endpoint service from on premises and from multiple VPCs within the company's AWS infrastructure.
Which combination of steps should the network engineer take to ensure that the client applications can resolve DNS for the interface endpoint? (Choose three.)

A. Create the interface endpoint for Amazon SQS with the option for private DNS names turned on.
B. Create the interface endpoint for Amazon SQS with the option for private DNS names turned off.
C. Manually create a private hosted zone for sqs.us-east-1.amazonaws.co
D. Add necessary records that point to the interface endpoin
E. Associate the private hosted zones with other VPCs.
F. Use the automatically created private hosted zone for sqs.us-east-1.amazonaws.com with previously created necessary records that point to the interface endpoin
G. Associate the private hosted zones with other VPCs.
H. Access the SQS endpoint by using the public DNS name sqs.us-east-1 amazonaws.com in VPCs and on premises.
I. Access the SQS endpoint by using the private DNS name of the interface endpoint.sqs.us-east-1.vpce.amazonaws.com in VPCs and on premises.

Answer: ADF

NEW QUESTION 43
A company has deployed its AWS environment in a single AWS Region. The environment consists of a few hundred application VPCs, a shared services VPC, and a VPN connection to the company's on-premises environment. A network engineer needs to implement a transit gateway with the following requirements:
• Application VPCs must be isolated from each other.
• Bidirectional communication must be allowed between the application VPCs and the on-premises network.
• Bidirectional communication must be allowed between the application VPCs and the shared services VPC. The network engineer creates the transit gateway with options disabled for default route table association and default route table propagation. The network engineer also creates the VPN attachment for the on-premises network and creates the VPC attachments for the application VPCs and the shared services VPC.
The network engineer must meet all the requirements for the transit gateway by designing a solution that needs the least number of transit gateway route tables.
Which combination of actions should the network engineer perform to accomplish this goal?(Choose two.)

A. Configure a separate transit gateway route table for on premise
B. Associate the VPN attachment with this transit gateway route tabl
C. Propagate all application VPC attachments to this transit gateway route table.
D. Configure a separate transit gateway route table for each application VP
E. Associate each application VPC attachment with its respective transit gateway route tabl
F. Propagate the shared services VPC attachment and the VPN attachment to this transit gateway route table.
G. Configure a separate transit gateway route table for all application VPC
H. Associate all application VPCs with this transit gateway route tabl
I. Propagate the shared services VPC attachment and the VPNattachment to this transit gateway route table.
J. Configure a separate transit gateway route table for the shared services VP
K. Associate the shared services VPC attachment with this transit gateway route tabl
L. Propagate all application VPC attachments to this transit gateway route table.
M. Configure a separate transit gateway route table for on premises and the shared services VP
N. Associate the VPN attachment and the shared services VPC attachment with this transit gateway route tabl
O. Propagate all application VPC attachments to this transit gateway route table.

Answer: BD

NEW QUESTION 44
A company has deployed a critical application on a fleet of Amazon EC2 instances behind an Application Load Balancer. The application must always be reachable on port 443 from the public internet. The application recently had an outage that resulted from an incorrect change to the EC2 security group.
A network engineer needs to automate a way to verify the network connectivity between the public internet and the EC2 instances whenever a change is made to the security group. The solution also must notify the network engineer when the change affects the connection.
Which solution will meet these requirements?

A. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture REJECT traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Log
B. Create a CloudWatch Logs metric filter for the log group for rejected traffi
C. Create an alarm to notify the network engineer.
D. Enable VPC Flow Logs on the elastic network interface of each EC2 instance to capture all traffic on port 443. Publish the flow log records to a log group in Amazon CloudWatch Log
E. Create a CloudWatch Logs metric filter for the log group for all traffi
F. Create an alarm to notify the network engineer
G. Create a VPC Reachability Analyzer path on port 443. Specify the security group as the sourc
H. Specify the EC2 instances as the destinatio
I. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connectio
J. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fail Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security groupoccurs.
K. Create a VPC Reachability Analyzer path on port 443. Specify the internet gateway of the VPC as the sourc
L. Specify the EC2 instances as the destinatio
M. Create an Amazon Simple Notification Service (Amazon SNS) topic to notify the network engineer when a change to the security group affects the connectio
N. Create an AWS Lambda function to start Reachability Analyzer and to publish a message to the SNS topic in case the analyses fai
O. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to invoke the Lambda function when a change to the security group occurs.

Answer: C

NEW QUESTION 45
A company has a global network and is using transit gateways to connect AWS Regions together. The company finds that two Amazon EC2 instances 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 table
B. Use VPC flow logs 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 are correc
D. Use AWS Firewall Manager to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.
E. Use AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables.Verify that the VPC route tables are correc
F. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.
G. Use VPC Reachability Analyzer to analyze routes in the transit gateway route table
H. Verify that the VPC route tables are correc
I. Use VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC.

Answer: C

Explanation:
Using AWS Network Manager Route Analyzer to analyze routes in the transit gateway route tables would enable identification of routing issues between VPCs and transit gateways1. Verifying that the VPC route tables are correct would enable identification of routing issues within a VPC. Using VPC flow logs to analyze the IP traffic that security group rules and network ACL rules accept or reject in the VPC would enable identification of traffic filtering issues within a VPC2. Additionally, using VPC Reachability Analyzer to analyze routes in the transit gateway route tables would enable identification of routing issues between transit gateways in different Regions. VPC Reachability Analyzer is a configuration analysis tool that enables connectivity testing between a source resource and a destination resource in your VPCs.

NEW QUESTION 48
An organization is using a VPC endpoint for Amazon S3. When the security group rules for a set of instances were initially configured, access was restricted to allow traffic only to the IP addresses of the Amazon S3 API endpoints in the region from the published JSON file. The application was working properly, but now is logging a growing number of timeouts when connecting with Amazon S3. No internet gateway is configured for the VPC.
Which solution will fix the connectivity failures with the LEAST amount of effort?

A. Create a Lambda function to update the security group based on AmazonIPSpaceChanged notifications.
B. Update the VPC routing to direct Amazon S3 prefix-list traffic to the VPC endpoint using the route table APIs.
C. Update the application server’s outbound security group to use the prefix-list for Amazon S3 in the same region.
D. Create an additional VPC endpoint for Amazon S3 in the same route table to scale the concurrent connections to Amazon.

Answer: C

Explanation:
https://aws.amazon.com/blogs/aws/subscribe-to-aws-public-ip-address-changes-via-amazon-sns/

NEW QUESTION 51
An organization launched an IPv6-only web portal to support IPv6-native mobile clients. Front-end instances launch in an Amazon VPC associated with an appropriate IPv6 CIDR. The VPC IPv4 CIDR is fully utilized. A single subnet exists in each of two Availability Zones with appropriately configured IPv6 CIDR associations. Auto Scaling is properly configured, and no Elastic Load Balancing is used.
Customers say the service is unavailable during peak load times. The network engineer attempts to launch an instance manually and receives the following message: “There are not enough free addresses in subnet ‘subnet-12345677’ to satisfy the requested number of instances.”
What action will resolve the availability problem?

A. Create a new subnet using a VPC secondary IPv6 CIDR, and associate an IPv6 CID
B. Include the new subnet in the Auto Scaling group.
C. Create a new subnet using a VPC secondary IPv4 CIDR, and associate an IPv6 CID
D. Include the new subnet in the Auto Scaling group.
E. Resize the IPv6 CIDR on each of the existing subnet
F. Modify the Auto Scaling group maximum number of instances.
G. Add a secondary IPv4 CIDR to the Amazon VP
H. Assign secondary IPv4 address space to each of theexisting subnets.

Answer: B

NEW QUESTION 54
A company hosts a web application on Amazon EC2 instances behind an Application Load Balancer (ALB). The ALB is the origin in an Amazon CloudFront distribution. The company wants to implement a custom authentication system that will provide a token for its authenticated customers.
The web application must ensure that the GET/POST requests come from authenticated customers before it delivers the content. A network engineer must design a solution that gives the web application the ability to identify authorized customers.
What is the MOST operationally efficient solution that meets these requirements?

A. Use the ALB to inspect the authorized token inside the GET/POST request payloa
B. Use an AWS Lambda function to insert a customized header to inform the web application of an authenticated customer request.
C. Integrate AWS WAF with the ALB to inspect the authorized token inside the GET/POST request payloa
D. Configure the ALB listener to insert a customized header to inform the web application of an authenticated customer request.
E. Use an AWS Lambda@Edge function to inspect the authorized token inside the GET/POST request payloa
F. Use the Lambda@Edge function also to insert a customized header to inform the web application of an authenticated customer request.
G. Set up an EC2 instance that has a third-party packet inspection tool to inspect the authorized token inside the GET/POST request payloa
H. Configure the tool to insert a customized header to inform the web application of an authenticated customer request.

Answer: C

NEW QUESTION 56
A company’s network engineer needs to design a new solution to help troubleshoot and detect network anomalies. The network engineer has configured Traffic Mirroring. However, the mirrored traffic is overwhelming the Amazon EC2 instance that is the traffic mirror target. The EC2 instance hosts tools that the company’s security team uses to analyze the traffic. The network engineer needs to design a highly available solution that can scale to meet the demand of the mirrored traffic.
Which solution will meet these requirements?

A. Deploy a Network Load Balancer (NLB) as the traffic mirror targe

B. Behind the NL
C. deploy a fleet of EC2 instances in an Auto Scaling grou
D. Use Traffic Mirroring as necessary.
E. Deploy an Application Load Balancer (ALB) as the traffic mirror targe
F. Behind the ALB, deploy a fleet of EC2 instances in an Auto Scaling grou
G. Use Traffic Mirroring only during non-business hours.
H. Deploy a Gateway Load Balancer (GLB) as the traffic mirror targe
I. Behind the GL
J. deploy a fleet of EC2 instances in an Auto Scaling grou
K. Use Traffic Mirroring as necessary.
L. Deploy an Application Load Balancer (ALB) with an HTTPS listener as the traffic mirror targe
M. Behind the AL
N. deploy a fleet of EC2 instances in an Auto Scaling grou
O. Use Traffic Mirroring only during active events or business hours.

Answer: A

NEW QUESTION 58
A company’s network engineer builds and tests network designs for VPCs in a development account. The company needs to monitor the changes that are made to network resources and must ensure strict compliance with network security policies. The company also needs access to the historical configurations of network resources.
Which solution will meet these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule with a custom pattern to monitor the account for change
B. Configure the rule to invoke an AWS Lambda function to identify noncompliant resource
C. Update an Amazon DynamoDB table with the changes that are identified.
D. Create custom metrics from Amazon CloudWatch log
E. Use the metrics to invoke an AWS Lambda function to identify noncompliant resource
F. Update an Amazon DynamoDB table with the changes that are identified.
G. Record the current state of network resources by using AWS Confi
H. Create rules that reflect the desired configuration setting
I. Set remediation for noncompliant resources.
J. Record the current state of network resources by using AWS Systems Manager Inventor
K. Use Systems Manager State Manager to enforce the desired configuration settings and to carry out remediation for noncompliant resources.

Answer: C

Explanation:
Recording the current state of network resources by using AWS Config would enable auditing and assessment of resource configurations and compliance3. Creating rules that reflect the desired configuration settings would enable evaluation of whether the network resources comply with network security policies3. Setting remediation for noncompliant resources would enable automatic correction of undesired configurations3.

NEW QUESTION 63
A company deploys a new web application on Amazon EC2 instances. The application runs in private subnets in three Availability Zones behind an Application Load Balancer (ALB). Security auditors require encryption of all connections. The company uses Amazon Route 53 for DNS and uses AWS Certificate Manager (ACM) to automate SSL/TLS certificate provisioning. SSL/TLS connections are terminated on the ALB.
The company tests the application with a single EC2 instance and does not observe any problems. However, after production deployment, users report that they can log in but that they cannot use the application. Every new web request restarts the login process.
What should a network engineer do to resolve this issue?

A. Modify the ALB listener configuratio
B. Edit the rule that forwards traffic to the target grou
C. Change the rule to enable group-level stickines
D. Set the duration to the maximum application session length.
E. Replace the ALB with a Network Load Balance
F. Create a TLS listene
G. Create a new target group with the protocol type set to TLS Register the EC2 instance
H. Modify the target group configuration by enabling the stickiness attribute.
I. Modify the ALB target group configuration by enabling the stickiness attribut
J. Use an application-based cooki
K. Set the duration to the maximum application session length.
L. Remove the AL
M. Create an Amazon Route 53 rule with a failover routing policy for the application nam
N. Configure ACM to issue certificates for each EC2 instance.

Answer: C

NEW QUESTION 64
A network engineer is designing a hybrid architecture that uses a 1 Gbps AWS Direct Connect connection between the company's data center and two AWS Regions: us-east-1 and eu-west-1. The VPCs in us-east-1 are connected by a transit gateway and need to access several on-premises databases. According to company policy, only one VPC in eu-west-1 can be connected to one on-premises server. The on-premises network segments the traffic between the databases and the server.
How should the network engineer set up the Direct Connect connection to meet these requirements?

A. Create one hosted connectio
B. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direc
C. Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.
D. Create one hosted connectio
E. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

F. Create one dedicated connectio
G. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use one Direct Connect gateway for both VIFs to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.
H. Create one dedicated connectio
I. Use a transit VIF to connect to the transit gateway in us-east-1. Use a private VIF to connect to the VPC in eu-west-1. Use two Direct Connect gateways, one for each VIF, to route from the Direct Connect locations to the corresponding AWS Region along the path that has the lowest latency.

Answer: B

Explanation:
This solution meets the requirements of the company by using a single Direct Connect connection with two VIFs, one connected to the transit gateway in us-east-1 and the other connected to the VPC in eu-west-1. Two Direct Connect gateways are used, one for each VIF, to route traffic from the Direct Connect location to the corresponding AWS Region along the path that has the lowest latency. This setup ensures that traffic between the VPCs in us-east-1 and on-premises databases is routed through the transit gateway, while traffic between the VPC in eu-west-1 and the on-premises server is routed directly through the private VIF.

NEW QUESTION 65
A company uses a 4 Gbps AWS Direct Connect dedicated connection with a link aggregation group (LAG) bundle to connect to five VPCs that are deployed in the us-east-1 Region. Each VPC serves a different business unit and uses its own private VIF for connectivity to the on-premises environment. Users are reporting slowness when they access resources that are hosted on AWS.
A network engineer finds that there are sudden increases in throughput and that the Direct Connect connection becomes saturated at the same time for about an hour each business day. The company wants to know which business unit is causing the sudden increase in throughput. The network engineer must find out this information and implement a solution to resolve the problem.
Which solution will meet these requirements?

A. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observe
B. Create a new 10 Gbps dedicated connectio
C. Shift traffic from the existing dedicated connection to the new dedicated connection.
D. Review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observe
E. Upgrade the bandwidth of the existing dedicated connection to 10 Gbps.
F. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observe
G. Upgrade the existing dedicated connection to a 5 Gbps hosted connection.
H. Review the Amazon CloudWatch metrics for ConnectionBpsIngress and ConnectionPpsEgress to determine which VIF is sending the highest throughput during the period in which slowness is observed.Create a new 10 Gbps dedicated connectio
I. Shift traffic from the existing dedicated connection to the new dedicated connection.

Answer: A

Explanation:
To meet the requirements of finding out which business unit is causing the sudden increase in throughput and resolving the problem, the network engineer should review the Amazon CloudWatch metrics for VirtualInterfaceBpsEgress and VirtualInterfaceBpsIngress to determine which VIF is sending the highest throughput during the period in which slowness is observed (Option B). After identifying the VIF that is causing the issue, they can upgrade the bandwidth of the existing dedicated connection to 10 Gbps to resolve the problem (Option B).

NEW QUESTION 70
A company has deployed an application in a VPC that uses a NAT gateway for outbound traffic to the internet. A network engineer notices a large quantity of suspicious network traffic that is traveling from the VPC over the internet to IP addresses that are included on a deny list. The network engineer must implement a solution to determine which AWS resources are generating the suspicious traffic. The solution must minimize cost and administrative overhead.
Which solution will meet these requirements?

A. Launch an Amazon EC2 instance in the VP
B. Use Traffic Mirroring by specifying the NAT gateway as the source and the EC2 instance as the destinatio
C. Analyze the captured traffic by using open-source tools to identify the AWS resources that are generating the suspicious traffic.
D. Use VPC flow log
E. Launch a security information and event management (SIEM) solution in the VP
F. Configure the SIEM solution to ingest the VPC flow log
G. Run queries on the SIEM solution to identify the AWS resources that are generating the suspicious traffic.
H. Use VPC flow log
I. Publish the flow logs to a log group in Amazon CloudWatch Log
J. Use CloudWatch Logs Insights to query the flow logs to identify the AWS resources that are generating the suspicious traffic.
K. Configure the VPC to stream the network traffic directly to an Amazon Kinesis data strea
L. Send the data from the Kinesis data stream to an Amazon Kinesis Data Firehose delivery stream to store the data in Amazon S3. Use Amazon Athena to query the data to identify the AWS resources that are generating the suspicious traffic.

Answer: C

NEW QUESTION 74
A company is developing an application in which IoT devices will report measurements to the AWS Cloud. The application will have millions of end users. The company observes that the IoT devices cannot support DNS resolution. The company needs to implement an Amazon EC2 Auto Scaling solution so that the IoT devices can connect to an application endpoint without using DNS.
Which solution will meet these requirements MOST cost-effectively?

A. Use an Application Load Balancer (ALB)-type target group for a Network Load Balancer (NLB). Create an EC2 Auto Scaling grou
B. Attach the Auto Scaling group to the AL
C. Set up the IoT devices to connect to the IP addresses of the NLB.
D. Use an AWS Global Accelerator accelerator with an Application Load Balancer (ALB) endpoin
E. Create an EC2 Auto Scaling grou
F. Attach the Auto Scaling group to the ALSet up the IoT devices to connect to the IP addresses of the accelerator.

G. Use a Network Load Balancer (NLB). Create an EC2 Auto Scaling grou
H. Attach the Auto Scaling group to the NL
I. Set up the IoT devices to connect to the IP addresses of the NLB.
J. Use an AWS Global Accelerator accelerator with a Network Load Balancer (NLB) endpoin
K. Create anEC2 Auto Scaling grou
L. Attach the Auto Scaling group to the NL
M. Set up the IoT devices to connect to the IP addresses of the accelerator.

Answer: D

Explanation:
AWS Global Accelerator can provide static IP addresses that the IoT devices can connect to without using DNS2. It can also route traffic over the AWS global network and improve performance and availability for the IoT devices2. An NLB can provide end-to-end encryption for HTTPS traffic by using TLS as a target group protocol and terminating SSL connections at the load balancer level1. An NLB can also support session affinity (sticky sessions) with TCP connections1.

NEW QUESTION 78
A company has multiple AWS accounts. Each account contains one or more VPCs. A new security guideline requires the inspection of all traffic between VPCs. The company has deployed a transit gateway that provides connectivity between all VPCs. The company also has deployed a shared services VPC with Amazon EC2 instances that include IDS services for stateful inspection. The EC2 instances are deployed across three Availability Zones. The company has set up VPC associations and routing on the transit gateway. The company has migrated a few test VPCs to the new solution for traffic inspection.
Soon after the configuration of routing, the company receives reports of intermittent connections for traffic that crosses Availability Zones.
What should a network engineer do to resolve this issue?

A. Modify the transit gateway VPC attachment on the shared services VPC by enabling cross-Availability Zone load balancing.
B. Modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support.
C. Modify the transit gateway by selecting VPN equal-cost multi-path (ECMP) routing support.
D. Modify the transit gateway by selecting multicast support.

Answer: B

Explanation:
To resolve the issue of intermittent connections for traffic that crosses Availability Zonesafter configuring routing for traffic inspection between VPCs using a transit gateway and EC2 instances with IDS services in a shared services VPC, a network engineer should modify the transit gateway VPC attachment on the shared services VPC by enabling appliance mode support (Option B). This will ensure that traffic is routed to the same EC2 instance for stateful inspection and prevent intermittent connections.

NEW QUESTION 81
A company is deploying a new application on AWS. The application uses dynamic multicasting. The company has five VPCs that are all attached to a transit gateway Amazon EC2 instances in each VPC need to be able to register dynamically to receive a multicast transmission.
How should a network engineer configure the AWS resources to meet these requirements?

A. Create a static source multicast domain within the transit gatewa
B. Associate the VPCs and applicable subnets with the multicast domai
C. Register the multicast senders' network interface with the multicast domai
D. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.
E. Create a static source multicast domain within the transit gatewa
F. Associate the VPCs and applicable subnets with the multicast domai
G. Register the multicast senders' network interface with the multicast domai
H. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.
I. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway.Associate the VPCs and applicable subnets with the multicast domai
J. Register the multicast senders' network interface with the multicast domai
K. Adjust the network ACLs to allow UDP traffic from the source to all receivers and to allow UDP traffic that is sent to the multicast group address.
L. Create an Internet Group Management Protocol (IGMP) multicast domain within the transit gateway.Associate the VPCs and applicable subnets with the multicast domai
M. Register the multicast senders' network interface with the multicast domai
N. Adjust the network ACLs to allow TCP traffic from the source to all receivers and to allow TCP traffic that is sent to the multicast group address.

Answer: C

NEW QUESTION 83
A company has several production applications across different accounts in the AWS Cloud. The company operates from the us-east-1 Region only. Only certain partner companies can access the applications. The applications are running on Amazon EC2 instances that are in an Auto Scaling group behind an Application Load Balancer (ALB). The EC2 instances are in private subnets and allow traffic only from the ALB. The ALB 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 is associated with the ALB in each account. A network engineer must implement a solution to centrally manage the partner network IP address ranges.
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 update
B. Update the DynamoDB table with the new IP address range when the company adds a new partne
C. Invoke an AWS Lambda function to read new IP address ranges and security groups from the DynamoDB table to update the security group
D. Deploy this solution in all accounts.
E. Create a new prefix lis
F. Add all allowed IP address ranges to the prefix lis
G. 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 lis
H. Deploy this solution in all accounts.
I. Create a new prefix lis
J. Add all allowed IP address ranges to the prefix lis

K. Share the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM). Update security groups to use the prefix list instead of the partner IP address rang
L. Update the prefix list with the new IP address range when the company adds a new partner.
M. Create an Amazon S3 bucket to maintain all IP address ranges and security groups that need to be update
N. Update the S3 bucket with the new IP address range when the company adds a new partne
O. Invoke an AWS Lambda function to read new IP address ranges and security groups from the S3 bucket to update the security group
P. Deploy this solution in all accounts.

Answer: C

Explanation:
Creating a new prefix list and adding all allowed IP address ranges to the prefix list would enable grouping of CIDR blocks that can be referenced in security group rules3. Sharing the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM)would enable central management of the partner network IP address ranges5. Updating security groups to use the prefix list instead of the partner IP address range would enable simplification of security group rules3. Updating the prefix list with the new IP address range when the company adds a new partner would enable automatic propagation of the changes to all security groups that use the prefix list3.

NEW QUESTION 84
A company uses a hybrid architecture and has an AWS Direct Connect connection between its on-premises data center and AWS. The company has production applications that run in the on-premises data center. The company also has production applications that run in a VPC. The applications that run in the on-premises data center need to communicate with the applications that run in the VPC. The company is using corp.example.com as the domain name for the on-premises resources and is using an Amazon Route 53 private hosted zone for aws.example.com to host the VPC resources.
The company is using an open-source recursive DNS resolver in a VPC subnet and is using a DNS resolver in the on-premises data center. The company's on-premises DNS resolver has a forwarder that directs requests for the aws.example.com domain name to the DNS resolver in the VPC. The DNS resolver in the VPC has a forwarder that directs requests for the corp.example.com domain name to the DNS resolver in the on-premises data center. The company has deckled to replace the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints.
Which combination of steps should a network engineer take to make this replacement? (Choose three.)

A. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the outbound endpoint.
B. Configure the on-premises DNS resolver to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.
C. Create a Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint.
D. Create a Route 53 Resolver rule to forward aws.example.com domain queries to the IP addresses of the inbound endpoint.
E. Create a Route 53 Resolver rule to forward corp.example.com domain queries to the IP address of the on-premises DNS resolver.
F. Configure the on-premises DNS resolver to forward aws.example.com queries to the IP addresses of the outbound endpoint.

Answer: BCE

Explanation:
To replace the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints in a hybrid architecture where on-premises applications need to communicate with applications running in a VPC, a network engineer should take the following steps:

- Create a Route 53 Resolver inbound endpoint and a Route 53 Resolver outbound endpoint. (Option C)
- Configure the on-premises DNS resolver to forward aws.example.com domain queries to the IP addresses of the inbound endpoint. (Option B)
- Create a Route 53 Resolver rule to forward corp.example.com domain queries to the IP address of the on-premises DNS resolver. (Option E)

These steps will allow for seamless replacement of the open-source recursive DNS resolver with Amazon Route 53 Resolver endpoints and enable communication between on-premises and VPC applications.

NEW QUESTION 89
A company uses AWS Direct Connect to connect its corporate network to multiple VPCs in the same AWS account and the same AWS Region. Each VPC uses its own private VIF and its own virtual LAN on the Direct Connect connection. The company has grown and will soon surpass the limit of VPCs and private VIFs for each connection.
What is the MOST scalable way to add VPCs with on-premises connectivity?

A. Provision a new Direct Connect connection to handle the additional VPC
B. Use the new connection to connect additional VPCs.
C. Create virtual private gateways for each VPC that is over the service quot
D. Use AWS Site-to-Site VPNto connect the virtual private gateways to the corporate network.
E. Create a Direct Connect gateway, and add virtual private gateway associations to the VPC
F. Configure a private VIF to connect to the corporate network.
G. Create a transit gateway, and attach the VPC
H. Create a Direct Connect gateway, and associate it with the transit gatewa
I. Create a transit VIF to the Direct Connect gateway.

Answer: D

Explanation:
When a company requires connectivity to multiple VPCs over AWS Direct Connect, a scalable solution is to use a transit gateway. A transit gateway is a hub that can interconnect multiple VPCs and VPN connections. The VPCs can communicate with each other over the transitgateway, and on-premises networks can communicate with the VPCs through the Direct Connect gateway. This solution provides a central point of management and simplifies the configuration of network routing. By associating the Direct Connect gateway with the transit gateway, traffic between the VPCs and the on-premises network can be routed through the Direct Connect connection.

NEW QUESTION 90
......