QUESTION 198
A company has a hybrid IT setup that includes services that run in an on-premises data center and in the AWS Cloud. The company is using AWS Direct Connect to connect its data center to AWS. The company is using one AWS Site-to-Site VPN connection as backup and requires a backup connectivity option to always be present. The company is transitioning to IPv6 by implementing dual-stack architectures.
Which combination of steps will transition the data center's connectivity to AWS in the LEAST amount of time? (Choose two.)

A. Create a new Site-to-Site VPN tunnel for the IPv6 traffic.
B. Create a new dual-stack Site-to-Site VPN connection between the data center and AWS. Provision routing. Delete the original Site-to-Site VPN connection.
C. Associate a new dual-stack public VIF with the Direct Connect connection. Migrate the Direct Connect traffic to the new VIF.
D. Add a new IPv6 peer in the existing VIF. Use the IPv6 address provided by Amazon on the peer router.
E. Send IPv6 traffic between the data center and AWS in a tunnel inside the existing IPv4 tunnels.

Answer: AD

QUESTION 199
A company is developing a new application that is deployed in multiple VPCs across multiple AWS Regions. The VPCs are connected through AWS Transit Gateway. The VPCs contain private subnets and public subnets.
All outbound internet traffic in the private subnets must be audited and logged. The company's network engineer plans to use AWS Network Firewall and must ensure that all traffic through Network Firewall is completely logged for auditing and alerting.
How should the network engineer configure Network Firewall logging to meet these requirements?

A. Configure Network Firewall logging in Amazon CloudWatch to capture all alerts. Send the logs to a log group in Amazon CloudWatch Logs.
B. Configure Network Firewall logging in Network Firewall to capture all alerts and flow logs.
C. Configure Network Firewall logging by configuring VPC Flow Logs for the firewall endpoint. Send the logs to a log group in Amazon CloudWatch Logs.
D. Configure Network Firewall logging by configuring AWS CloudTrail to capture data events.

Answer: B

QUESTION 200
A company has set up a NAT gateway in a single Availability Zone (AZ1) in a VPC (VPC1) to access the internet from Amazon EC2 workloads in the VPC. The EC2 workloads are running in private subnets in three Availability Zones (AZ1, AZ2, AZ3). The route table for each subnet is configured to use the NAT gateway to access the internet.
Recently during an outage, internet access stopped working for the EC2 workloads because of the NAT gateway's

unavailability. A network engineer must implement a solution to remove the single point of failure from the architecture and provide built-in redundancy.
Which solution will meet these requirements?

A. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table for private subnets to route traffic to the virtual IP addresses of the two NAT gateways.
B. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table to point the AZ2 private subnets to the NAT gateway in AZ2. Configure the same route table to point the AZ3 private subnets to the NAT gateway in AZ3.
C. Create a second VPC (VPC2). Set up two NAT gateways. Place each NAT gateway in a different VPC (VPC1 and VPC2) and in the same Availability Zone (AZ2). Configure a route table in VPC1 to point the AZ2 private subnets to one NAT gateway. Configure a route table in VPC2 to point the AZ2 private subnets to the second NAT gateway.
D. Set up two NAT gateways. Place each NAT gateway in a different public subnet in separate Availability Zones (AZ2 and AZ3). Configure a route table to point the AZ2 private subnets to the NAT gateway in AZ2. Configure a second route table to point the AZ3 private subnets to the NAT gateway in AZ3.

Answer: D

QUESTION 201
A company has a total of 30 VPCs. Three AWS Regions each contain 10 VPCs. The company has attached the VPCs in each Region to a transit gateway in that Region. The company also has set up inter-Region peering connections between the transit gateways.
The company wants to use AWS Direct Connect to provide access from its on-premises location for only four VPCs across the three Regions. The company has provisioned four Direct Connect connections at two Direct Connect locations.
Which combination of steps will meet these requirements MOST cost-effectively? (Choose three.)

A. Create four virtual private gateways. Attach the virtual private gateways to the four VPCs.
B. Create a Direct Connect gateway. Associate the four virtual private gateways with the Direct Connect gateway.
C. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the Direct Connect gateway.
D. Create four transit VIFs on each Direct Connect connection. Associate the transit VIFs with the four virtual private gateways.
E. Create four private VIFs on each Direct Connect connection to the Direct Connect gateway.
F. Create an association between the Direct Connect gateway and the transit gateways.

Answer: ABE
Explanation:
TGW for inter VPC peering within AWS. From on-prem access to only 4 VPCs is required. Hence DXGW and VGW via private VIF. Peering TGW with DXGW would be possible for on-prem connectivity but is more costly.
https://docs.aws.amazon.com/whitepapers/latest/hybrid-connectivity/aws-dx-dxgw-with-vgw-multi-regions-and-aws-public-peering.html

QUESTION 202
A company needs to manage Amazon EC2 instances through command line interfaces for Linux hosts and Windows hosts. The EC2 instances are deployed in an environment in which there is no route to the internet. The company must implement role-based access control for management of the instances. The company has a standalone on-premises environment.
Which approach will meet these requirements with the LEAST maintenance overhead?

A. Set up an AWS Direct Connect connection between the on-premises environment and the VPC where the instances are deployed. Configure routing, security groups, and ACLs. Connect to the

instances by using the Direct Connect connection.

B. Deploy and configure AWS Systems Manager Agent (SSM Agent) on each instance. Deploy VPC endpoints for Systems Manager Session Manager. Connect to the instances by using Session Manager.

C. Establish an AWS Site-to-Site VPN connection between the on-premises environment and the VPC where the instances are deployed. Configure routing, security groups, and ACLs. Connect to the instances by using the Site-to-Site VPN connection.

D. Deploy an appliance to the VPC where the instances are deployed. Assign a public IP address to the appliance. Configure security groups and ACLs. Connect to the instances by using the appliance as an intermediary.

Answer: B

QUESTION 203

A network engineer needs to improve the network security of an existing AWS environment by adding an AWS Network Firewall firewall to control internet-bound traffic. The AWS environment consists of five VPCs. Each VPC has an internet gateway, NAT gateways, public Application Load Balancers (ALBs), and Amazon EC2 instances. The EC2 instances are deployed in private subnets. The architecture is deployed across two Availability Zones.

The network engineer must be able to configure rules for the public IP addresses in the environment, regardless of the direction of traffic. The network engineer must add the firewall by implementing a solution that minimizes changes to the existing production environment. The solution also must ensure high availability.

Which combination of steps should the network engineer take to meet these requirements? (Choose two.)

A. Create a centralized inspection VPC with subnets in two Availability Zones. Deploy Network Firewall in this inspection VPC with an endpoint in each Availability Zone.

B. Configure new subnets in two Availability Zones in each VPC. Deploy Network Firewall in each VPC with an endpoint in each Availability Zone.

C. Deploy Network Firewall in each VPUse existing subnets in each of the two Availability Zones to deploy Network Firewall endpoints.

D. Update the route tables that are associated with the private subnets that host the EC2 instances. Add routes to the Network Firewall endpoints.

E. Update the route tables that are associated with the public subnets that host the NAT gateways and the ALBs. Add routes to the Network Firewall endpoints.

Answer: BE

QUESTION 204

A company is planning to migrate an internal application to the AWS Cloud. The application will run on Amazon EC2 instances in one VPC. Users will access the application from the company's on-premises data center through AWS VPN or AWS Direct Connect. Users will use private domain names for the application endpoint from a domain name that is reserved explicitly for use in the AWS Cloud.

Each EC2 instance must have automatic failover to another EC2 instance in the same AWS account and the same VPC. A network engineer must design a DNS solution that will not expose the application to the internet.

Which solution will meet these requirements?

A. Assign public IP addresses to the EC2 instances. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPC. Create a Route 53 Resolver outbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the outbound endpoint IP address for Route 53 Resolver. In the private hosted zone, configure primary and failover records that point to the public IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint.

B. Place the EC2 instances in private subnets. Create an Amazon Route 53 public hosted zone for the AWS reserved domain name. Associate the public hosted zone with the VPC. Create a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for

Route 53 Resolver. In the public hosted zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint.

C. Place the EC2 instances in private subnets. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPCreate a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for Route 53 Resolver. In the private hosted zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Create an Amazon CloudWatch metric and alarm to monitor the application's health. Set up a health check on the alarm for the primary application endpoint.

D. Place the EC2 instances in private subnets. Create an Amazon Route 53 private hosted zone for the AWS reserved domain name. Associate the private hosted zone with the VPC. Create a Route 53 Resolver inbound endpoint. Configure conditional forwarding in the on-premises DNS resolvers to forward all DNS queries for the AWS domain to the inbound endpoint IP address for Route 53 Resolver. In the private hosted zone, configure primary and failover records that point to the IP addresses of the EC2 instances. Set up Route 53 health checks on the private IP addresses of the EC2 instances.

Answer: C

QUESTION 205
A company uses Amazon Route 53 for its DNS needs. The company's security team wants to update the DNS infrastructure to provide the most recent security posture.
The security team has configured DNS Security Extensions (DNSSEC) for the domain. The security team wants a network engineer to explain who is responsible for the rotation of DNSSEC keys.
Which explanation should the network administrator provide to the security team?

A. AWS rotates the zone-signing key (ZSK). The company rotates the key-signing key (KSK).
B. The company rotates the zone-signing key (ZSK) and the key-signing key (KSK).
C. AWS rotates the AWS Key Management Service (AWS KMS) key and the key-signing key (KSK).
D. The company rotates the AWS Key Management Service (AWS KMS) key. AWS rotates the key-signing key (KSK).

Answer: A
Explanation:
You are responsible for KSK management, which includes rotating it if needed. ZSK management is performed by Route 53.
https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/dns-configuring-dnssec.html

QUESTION 206
A company has agreed to collaborate with a partner for a research project. The company has multiple VPCs in the us-east-1 Region that use CIDR blocks within 10.10.0.0/16. The VPCs are connected by a transit gateway that is named TGW-C in us-east-1. TGW-C has an Autonomous System Number (ASN) configuration value of 64520.
The partner has multiple VPCs in us-east-1 that use CIDR blocks within 172.16.0.0/16. The VPCs are connected by a transit gateway that is named TGW-P in us-east-1. TGW-P has an ASN configuration value of 64530.
A network engineer needs to establish network connectivity between the company's VPCs and the partner's VPCs in us-east-1.
Which solution will meet these requirements with MINIMUM changes to both networks?

A. Create a new VPC in a new account. Deploy a router from AWS Marketplace. Share TGW-C and TGW-P with the new account by using AWS Resource Access Manager (AWS RAM). Associate TGW-C and TGW-P with the new VPC. Configure the router in the new VPC to route between TGW-C and TGW-P.
B. Create an IPsec VPN connection between TGW-C and TGW-P. Configure the routing between the transit gateways to use the IPsec VPN connection.

C. Configure a cross-account transit gateway peering attachment between TGW-C and TGW-P. Configure the routing between the transit gateways to use the peering attachment.
D. Share TGW-C with the partner account by using AWS Resource Access Manager (AWS RAM). Associate the partner VPCs with TGW-C. Configure routing in the partner VPCs and TGW-C.

Answer: C

QUESTION 207
A company has a public application. The application uses an Application Load Balancer (ALB) that has a target group of Amazon EC2 instances.
The company wants to protect the application from security issues in web requests. The traffic to the application must have end-to-end encryption.
Which solution will meet these requirements?

A. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate on the EC2 instances that use a public certificate. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.
B. Configure TLS connections to terminate at the ALB that uses a public certificate. Configure AWS Certificate Manager (ACM) certificates for the communication between the ALB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the ALB.
C. Configure a Network Load Balancer (NLB) that has a target group of the existing EC2 instances. Configure TLS connections to terminate at the EC2 instances by creating a TLS listener. Configure self-signed certificates on the EC2 instances for the communication between the NLB and the EC2 instances. Configure an AWS WAF web ACL. Associate the web ACL with the NLB.
D. Configure a third-party certificate on the EC2 instances for the communication between the ALB and the EC2 instances. Import the third-party certificate into AWS Certificate Manager (ACM). Associate the imported certificate with the ALB. Configure TLS connections to terminate at the ALB. Configure an AWS WAF web ACL. Associate the web ACL with the ALB.

Answer: D

QUESTION 208
A company has an application that hosts personally identifiable information (PII) of users. All connections to the application must be secured by HTTPS with TLS certificates that implement Elliptic Curve Cryptography (ECC). The application uses stateful connections between the web tier and the end users. Multiple instances host the application. A network engineer must implement a solution that offloads TLS connections to a load balancer.
Which load-balancing solution will meet these requirements?

A. Provision a Network Load Balancer. Configure a TLS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS identity and Access Management (IAM). Turn on health checks to monitor the web hosts that connect to the end users.
B. Provision an Application Load Balancer. Configure an HTTPS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Certificate Manager (ACM). Configure a default action to redirect to the URL for the application. Turn on health checks to monitor the web hosts that connect to the end users.
C. Provision a Network Load Balancer. Configure a TLS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Certificate Manager (ACM). Turn on application-based session affinity (sticky sessions). Turn on health checks to monitor the web hosts that connect to the end users.
D. Provision an Application Load Balancer. Configure an HTTPS listener by specifying the use of an ECC SSL certificate that is uploaded to AWS Identity and Access Management (IAM). Configure a default action to redirect to the URL for the application. Turn on application-based session affinity (sticky sessions).

Answer: C

QUESTION 209

A company hosts infrastructure services in multiple VPCs across multiple accounts in the us-west-2 Region. The VPC CIDR blocks do not overlap. The company wants to connect the VPCs to its data centers by using AWS Site-to-Site VPN tunnels.
The connections must be encrypted in transit. Additionally, the connection from each data center must route to the closest AWS edge location. The connections must be highly available and must accommodate automatic failover.
Which solution will meet these requirements?

A. Deploy a transit gateway. Share the transit gateway with each of the other accounts by using AWS Resource Access Manager (AWS RAM). Create VPC attachments to the transit gateway from each service account. Add routes to the on-premises subnet in each of the service VPC route tables by using the attachment as the gateway. Create Site-to-Site VPN tunnel attachments with dynamic routing to the transit gateway. Enable the acceleration feature for the Site-to-Site VPN connection. Configure the VPN tunnels on the on-premises equipment. Configure BGP peering.
B. Deploy VPN gateways to each account. Enable the acceleration feature for VPN gateways on each account. Add routes to the on-premises subnet in each of the service VPC route tables. Use the VPNs as the gateway. Configure the VPN tunnels on the on-premises equipment. Configure BGP peering.
C. Deploy a transit gateway. Share the transit gateway with each of the other accounts by using AWS Resource Access Manager (AWS RAM). Create VPC attachments to the transit gateway from each service account. Add routes to the on-premises subnet in each of the service VPC route tables by using the attachment as the gateway. Create Site-to-Site VPN tunnel attachments with dynamic routing to the transit gateway. Enable the acceleration feature for the Site-to-Site VPN connection. Configure the VPN tunnels on the on-premises equipment. Configure static routing.
D. Deploy VPN gateways to each account. Enable the acceleration feature for VPN gateways on each account. Add routes to the on-premises subnet in each of the service VPC route tables. Use the VPNs as the gateway. Configure the VPN tunnels on the on-premises equipment. Configure static routing.

Answer: A

QUESTION 210
A company has a transit gateway in AWS Account A. The company uses AWS Resource Access Manager (AWS RAM) to share the transit gateway so that users in other accounts can connect to multiple VPCs in the same AWS Region.
AWS Account B contains a VPC (10.0.0.0/16) with subnet 10.0.0.0/24 in the us-west-2a Availability Zone and subnet 10.0.1.0/24 in the us-west-2b Availability Zone. Resources in these subnets can communicate with other VPCs.
A network engineer creates two new subnets: 10.0.2.0/24 in the us-west-2b Availability Zone and 10.0.3.0/24 in the us-west-2c Availability Zone. All the subnets share one route table. The default route 0.0.0.0/0 is pointing to the transit gateway. Resources in subnet 10.0.2.0/24 can communicate with other VPCs, but resources in subnet 10.0.3.0/24 cannot communicate with other VPCs.
What should the network engineer do so that resources in subnet 10.0.3.0/24 can communicate with other VPCs?

A. In Account B, add 10.0.2.0/24 and 10.0.3.0/24 as the destinations to the route table. Use the transit gateway as the target.
B. In Account B, update the transit gateway attachment. Attach the new subnet ID that is associated with us-west-2c to Account B's VPC.
C. In Account A, create a static route for 10.0.3.0/24 in the transit gateway route tables.
D. In Account A, recreate propagation for 10.0.0.0/16 in the transit gateway route tables.

Answer: B

QUESTION 211
A company has started using AWS Cloud WAN with one edge location in the us-east-1 Region. The company has a production segment and a security segment in AWS Cloud WAN. The company also has a default core network policy. The company has created a production VPC for the production workload. The company has created an outbound inspection VPC to inspect internet-bound traffic from the production VPC. The company has attached the production

VPC to the production segment and has attached the outbound inspection VPC to the security segment. The company has also created an AWS Network Firewall firewall in the outbound inspection VPC to inspect internet-based traffic. The company has updated a route table for the production VPC to send all internet-bound traffic to the AWS Cloud WAN core network. The company has updated a route table for the outbound inspection VPC to ensure that Network Firewall inspects any outgoing traffic and incoming traffic.
During testing, an Amazon EC2 instance in the production VPC cannot reach the internet. The company checks the Network Firewall rules and confirms that the rules are not blocking the traffic.
Which combination of steps will meet these requirements? (Choose two.)

A. Update the core network policy to configure segment sharing. Share the production segment with the security segment.
B. Update the core network policy to create a static route for the security segment. Specify 0.0.0.0/0 as the destination CIDR block. Specify the outbound inspection VPC as an attachment.
C. Update the core network policy to create a static route for the production segment. Specify 0.0.0.0/0 as the destination CIDR block. Specify the outbound inspection VPC as an attachment.
D. Update the core network policy to create a static route for the production segment. Specify 10.2.0.0/16 as the destination CIDR block. Specify the outbound inspection VPC as an attachment.
E. Create an attachment to attach the outbound inspection VPC to the production segment. Update the core network policy to turn on isolated attachment for the production segment.

Answer: AC