Answer Sheet

Q1)

TPT Limited wants to set up an AWS Direct Connect connection along with a private virtual interface. TPT Limited has 169 IP prefixes to be advertised via the private virtual interface. TPT Limited has made the request and made sure the equipment are in place.

Which implementation step will ensure the connection works as per the requirement?

● Ensure a VPC Peering connection is in place
● Create a VPN connection
● Ensure to also create a public VIF to access the resources in the VPC
✓ Summarize the routes into a default route
● None of these

Q2)

You're in charge for setting up the AWS Direct Connect connection between your onpremise data center and an AWS Partner location.

You need to ensure that your network can support the connection.

What needs to be In check for this. Choose 3 answers from the options given below

✓ The network device must support BGP
✓ Auto-negotiation for the port must be disabled for the network device
✓ The network must have support for 802.1Q VLAN
● The network device must support Static Routing

Q3)

Your company is planning on setting up a VPN connection between a VPC hosted in AWS and their on premise data center.

There is a need to ensure the VPN connection is highly available and at the same time to ensure cost is kept to a minimum.

What would you do to ensure these requirements are kept?

✓ VPN connections are already high available
● Create an additional VPC peering connection
● Create 2 VPN connections for high availability
● Create an additional Direct connect connection

Q4)

A company is planning to setup an AWS Direct Connect connection to access resources in AWS via their on- premise data center. They are estimating the costs that would be involved.

Which of the following should be taken Into account from a costing aspect for AWS Direct Connect? Choose 3 answers from the options given below

✓ Data transfer from a VPC via a private VIF
✓ Number of port hours consumed
● Data transfer into AWS Direct Connect
✓ Data transfer from a 53 bucket via a public V1F

Q5)

You are designing an online shopping application for your company. This application will be running in a VPC on EC2 instances behind an Application Load Balancer. The Instances run in an Auto Scaling group across multiple Availability Zones.

The application tier must read and write data to a customer managed database cluster. There should be no access to the database from the Internet, but the cluster must be able to obtain software patches from the Internet.

Which VPC design meets these requirements completely?

● Public subnets for the application tier, and private subnets for the database cluster and NAT Gateway
● Public subnets for the application tier, and private subnets for the database cluster and NAT gateway
● Public subnets for both the application tier and the database cluster
✓ Public subnets for the application tier and NAT Gateway. and private subnets for the database cluster

Q6)

An architecture consists of the following

a) A primary and secondary infrastructure hosted in AWS.

b) Both infrastructures consists of ELB, Auto scaling and EC2 resources

How should Route53 be configured to ensure proper failover incase the primary infrastructure goes down.

● Configure a weighted routing policy
✓ Configure a failover routing policy

- ● Configure a Multi-Answer routing policy
- ● Configure a primary routing policy

Q7)

Your company has setup a Cloud front distribution. They are using multiple EC2 Instances as the origin.

There is a requirement to ensure that cookies can be monitored in the requests.

Based on the cookies, different sites can be relayed back to the users.

Which of the following would help fulfill this requirement?

- ● Consider using RTMP distributions
- ● Consider using multiple origins
- ● Consider using proxy protocol
- ✓ Consider using Lambda at the edge

Q8)

A company has a requirement to send large amounts of data that needs to be ingested into S3. This needs to be done on a regular basis.

Also the data transfer needs to be encrypted. The data transfer line needs to be low latency and dependable.

How could you accomplish this?

- ● Use an AWS Direct Connect connection
- ● Use AWS Direct Connect over an AWS Managed VPN
- ✓ Use an AWS Managed VPN over AWS Direct Connect .
- ● Use an AWS VPN Managed connection

Q9)

Your company is planning on hosting an application on a set of EC2 Instances.

There is a requirement for complete end to end encryption for the data to ensure that the application is (HIPAA) compliant.

How can you achieve this?

- ● Ensure that the traffic is encrypted using KMS
- ● Setup a Direct Connect connection between the EC2 Instance and the Internet
- ● Setup a VPN connection between the EC2 Instance and the Internet
- ✓ Use SSL to encrypt all the data at the application layer

Q10)

Your team is planning on hosting an application in AWS. This application will be using a My SQL database hosted on an EC2 Instance.

It is anticipated that the disk performance might take a hit due to the high Input/ Output activity.

How can you ensure baseline performance with low latency for the database tier?

- ✓ Ensure to use EBS lops volumes
- ● Ensure to use Amazon S3 for storage
- ● Ensure to use the EFS file system
- ● Ensure to use an Instance with Enhanced Networking enabled

Q11)

Your production team had earlier created a VPC with the CIDR block of 192.168.0.0./i 6. Instances were launched in the VPC.

Now there is a decision to ensure the instances have an address space for 10.0.0.0/16. How can this be achieved?

- ● Add a new address space to the VPC. Then ensure that the instances use the new address space
- ✓ Create a new VPC with the address block of 10.0.0.0/16. Migrate all of the instances to the new VPC.
- ● Change the address block of the VPC from 192.168.0.0.116 to 10.0.0.0/1 6. All of the instances will now use the new address space.
- ● Launch a NAT Instance. Ensure that the instance performs Network address translation onto the CIDR range of 10.0.0.0/16

Q12)

Your company needs to create its own VPN based EC2 Instances. These Instances will allow 2 VPC's in different regions to talk to each other.

You've created one VPN Instance In one subnet in one VPC and another Instance in another subnet in another VPC.

You are establishing the communication via Internet gateway. What extra consideration should be in place in such a configuration?

- ✓ Having multiple VPN Instances for high availability
- ● Placing a Virtual private gateway as the termination endpoint
- ● Placing a NAT Instance in front of both of the VPN connections

● Using a Private hosted zone in Route 53

Q13)

You have created a VPC Endpoint for your private subnet to S3. The default endpoint policy is in place.

You are trying to access a bucket, but you're getting an access denied error. What must be done. Please select:

✓ Add the VPC Endpoint to the S3 bucket policy
● Add the VPC endpoint to the Bucket ACL
● Add the VPC endpoint to the Endpoint policy to allow access to the S3 bucket
● Add the VPC to the 53 bucket policy

Q14)

You have created an Application Load Balancer.

You need to point your domain names of www.example.com and example.com to the Application Load Balancer.

Your Hosted zone is example.com. How can you achieve this?

✓ Create an Alias record for example.com and point it to the ELB as the target. Create a CNAME record for www.example.com and point it to example.com
● Create one CNAME record for the ELB to www.example.com. And then create another CNAME record to the ELB to example.com
● Create an ALIAS record for the ELB and point it to example.com. Create a PTR record for www.example.cc and point it to exam ple.com
● Create one CNAME record for the ELB to www.example.com. And then create another PTR record to the E to example.com

Q15)

Your company has a department that has set their own AWS account that is not part of the consolidating billing process for the company.

They have setup a AWS Direct connect connection to a VPC via a Private VI They are downloading data from an EC2 Instance in the VPC.

How would the charges come across?

● The company would be charged for data transfer out via the Internet gateway
● The company would be charged for data transfer out via AWS Direct Connect
● The department would be charged for data transfer out via the Internet gateway
✓ The department would be charged for data transfer out via AWS Direct Connect

Q16)

Your company is planning on hosting an Active Directory Domain server in a VPC.

Resources in other VPC, will need to access the domain server for authentication and DNS routing.

What Is the core implementation steps you would consider In such a design? Choose 2 answers from the options given below?

● Consider a Transit VPC Design
● Make use of a VPN connection
✓ Consider a Hub and Spoke Model VPC Design
✓ Make use of VPC peering

Q17)

An organization is planning to setup a management network on the AWS VPC. The organization is trying to secure the web server on a single VPC instance such that it allows the internet traffic as well as the back-end management traffic.

The organization wants to make so that the back-end management network interface can receive the SSH traffic only from a selected IP range, while the internet facing web server will have an IP address which can receive traffic from all the internet IPs.

How can the organization achieve this by running web server on a single Instance?

● The organization should create 2 EC2 instances as this is not possible with one EC2 instance
● This Is not possible
✓ The organization should create 2 network Interfaces, one for the internet traffic and the other for the backend traffic
● It is not possible to have 2 IP addresses for a single instance

Q18)

You have been put in charge for setting up a network architecture for a company.

The architecture consists of an application that will exchange a lot of information and hence will need a high bandwidth consideration.

There will be other B2B customers that will access this application as separate tenants.

What consideration will you provide in the design?

● Allow each customer to connect via the Internet. Setup the right security groups and NACL?s for the application.

✓ Consider using AWS Direct Connect for each customer. But this will also depend on the availability of an AWS partner in that location of the customer.
● Consider using a Virtual private gateway for each customer as this will provide the least latency
● Consider using AWS VPN for each customer. But this will also depend on the availability of an AWS partner in that location of the customer.

Q19)

You have an EC2 Instance which will be responsible for processing a lot of video and audio.

There is a requirement to ensure that the EC2 Instance has the maximum performance when it comes to the network packet processing.

How can this be achieved? Choose 2 answers from the options given below

● Ensure that the MTU is set to 9001 for the VPC
✓ Ensure that the instance supports single root I/O virtualization
✓ Ensure that the MTU is set to 9001 on the Instance
● Choose a t2.medlum instance type

Q20)

You are planning on creating a fault tolerant EC2 Instance by creating a secondary network interface and a backup EC2 Instance.

Which of the following is a requirement to ensure the switch over can be done Qu successfully?

Choose 2 answers from the options given below ?

● The network Interface must reside In a different Availability Zone
✓ The network interface must reside in the same Availability Zone Sh
● The instance must reside in a different Availability Zone
✓ The instance must reside in the same Availability Zone

Q21)

You work for your company as an AWS administrator. You've setup a Classic Load balancer and EC2 Instances for an application. You have setup HTTPS listeners with the default security policies.

Your Security department has mentioned that the security policy defined for the load balancer does not meet the regulations defined for the policy.

What changes would you make to be in line with the requirements of the IT security department?

● Create a new SSL and associate it with the underlying Classic Load balancer
● Create a custom security policy and associate it with the EC2 Instance
● Create a new SSL and associate it with the underlying EC2 Instances
✓ Create a custom security policy and associate it with the Classic Load Balancer

Q22)

Your company has setup a host of networking components in AWS. They have out stringent controls in place to ensure that these networking components are only changed by designated IT personnel.

But they still need to get notified of any unwarranted access on networking components.

Which of the following service can help in this requirement?

● AWS Trusted Advisor
● AWS Inspector
● AWS VPC Flow Logs
✓ AWS Cloud trail

Q23)

You've setup an a Classic Load Balancer and EC2 Instances behind the Load Balancer.

The following Security Groups have been set

Security Group for the ELB - Accept Incoming traffic on port 80 from 0.0.0.0/0

Security Group for the EC2 Instances - Accept Incoming traffic on port 80 from 0.0.0.0/0 It has been noticed that the EC2 Instances are getting a large number of direct requests from the Internet.

What should be done to resolve the issue?

● Change the ELB security group to only accept traffic from the EC2 Instances on port 443
● Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 443
● Change the ELB security group to only accept traffic from the EC2 Instances on port 80
✓ Change the EC2 Instance security group to only accept traffic from the ELB Security Group on port 80

Q24)

Your company needs VPN connectivity to an AWS VPC.

There are around 100 mobile devices, 40 remote computers and a site office which needs to connect. How would you achieve this connectivity?

Choose 2 answers from the options given below

- ✓ Use a custom VPN server to accept connections from the mobile and remote computers
- ✓ Use AWS Managed VPN for the site office
- ● Use AWS Managed VPN for the mobile and remote computers
- ● Use AWS Direct Connect with a public VIF for the site office

Q25)

Your company has many VPC's , one for Development, one for Staging, one for Production and one Management VPC.

It is required for traffic to flow from the other VPC's to the Management VPC's. The VPC's should also be traversable via the on-premise Infrastructure.

How would you architect the solution with the least amount of effort?

- ● Creating a VPC peering connection between the VPCS. Create a VPN connection between the Management VPC and the on-premise environment.
- ✓ Creating a VPC peering connection between the VPC's. Create a VPN connection between all the VPC's and the on-premise environment.
- ● Create a Virtual Private gateway connection between all of the VPC's. Create a VPN connection between Management VPC and the on-premise environment.
- ● Create a VPN connection between the Management VPC and all other VPC5. Create a VPN connection between the Management VPC and the on-premise environment.

Q26)

Your company has created an AWS Direct Connect connection. A virtual private gateway is attached to a VPC.

Around 111 routes are being advertised on from On-premise. A private VIF Is being created to the VPGW.

But the Virtual Interface Is always showing as down.

What needs to be done to ensure the Interface comes back up?

- ● Ensure that the P sec configuration is correct
- ● Ensure that static routes are put in place
- ✓ Ensure less routes are being advertised.
- ● Ensure that a VPN connection Is also in place for the tunnel to become active.

Q27)

Your company has many remote branch offices that need to connect with your AWS VPC.

Which of the following can help achieve this connectivity in an easy manner?

- ● AWS Direct Connect with a Private VIF
- ✓ VPN Cloud hub
- ● AWS Direct Connect with a Public VIF
- ● VPC Peering

Q28)

A company has an application that needs to be moved to an AWS VPC network.

This application is based on multicast and needs to be moved with the least amount of effort.

What can be done to fulfill this requirement?

- ● Consider enabling encryption on the underlying EBS volumes which will be used to support the EC2
- ● The application needs to be changed to support uni cast before moving it to AWS.
- ● Create EC2 Instances in the subnet and then migrate the application on to the EC2 Instance.
- ✓ Consider creating an overlay network between EC2 Instances and then port the application.

Q29) When creating an AWS workspace, which of the following is required for the creation of the workspace?

- ● A NAT Instance on the customer side
- ● A VPC with a private and public subnet
- ✓ A User directory
- ● An AWS Direct Connect connection

Q30)

Your company has the following setup in AWS a. A set of EC2 Instances hosting a web application b.

An application load balancer placed in front of the EC2 Instances There seems to be a set of malicious requests coming from a set of IP addresses.

Which of the following can be used to protect against these requests?

● Use VPC Flow Logs to block the IP addresses
✓ Use AWS WAF to block the PP addresses
● Use AWS Inspector to block the IP addresses
● Use Security Groups to block the IP addresses

Q31)

Your company is planning on delivering content via an application hosted on a set of EC2 Instances.

The end devices can be laptops, mobile devices, tablets etc. The content needs to be customized based on the type of end user device.

Which of the following can help fulfill this requirement and also ensure that cost is MINIMIZED and MAXIMUM ease of deployment?

✓ Application Load Balancers
● App stream
✓ Cloud front with Lambda @Edge
● Network Load Balancers

Q32)

You are planning on using VPC Flow logs to monitor the traffic to EC2 Instances in your VPC.

Which of the following types of traffic will not get monitored by VPC Flow logs. Choose 2 answers from the options given below

● Traffic that flow to Amazon DNS servers
✓ Requests for Instance metadata
● Instances which have multiple ENrs
● Instances that have Elastic IP's assigned to the ENI

Q33)

Your company has a 3 tier application that consists of a Web , Application and Database Tier. The application is based on delivering REST full services.

They have Auto scaling Groups for the EC2 Instances for the Web and Application Tier.

You now want to add high availability to the Tiers, but it needs to ensured that each tier can be scaled independently.

How would you architect. Choose the most PREFERRED option.

● Create a Classic Load Balancer and add multiple targets for the Web and Application Tier.
● Create an Application Load Balancer for the Application Tier and a classic load balancer for the Web Tier
✓ Create an Application Load Balancer and add separate target groups for the Web and Application Tier
● Create separate Classic Load Balancers for the Web and Application Tiers.

Q34)

You've setup a Cloud front distribution in AWS. You're planning on conducting a primary load test to see the performance of the Cloud front distribution.

Which of the following factors must you keep in mind when performing the load test. Choose 2 answers from the options given below ?

● Ensure that client requests hit the origin server
✓ Configure your test so each client makes an independent DNS request
● Ensure that SSL is turned on for the distribution
✓ Ensure to initiate client requests from multiple geographic regions

Q35)

You need to setup a Cross Connect with AWS Direct Connect. You already have the necessary equipment in place.

You now need to complete the connection process. How can you achieve this?

✓ Contact your provider
● Raise a AWS Direct Connect request In the AWS Console
● Raise a support ticket with AWS
● Contact an AWS Partner

Q36)

A company currently has acquired another smaller company. Both companies have their presence in AWS.

There is a requirement to ensure traffic flows from VPC A in the parent company to a security VPC B in the same parent company.

And then the traffic can flow to VPC C in the acquired company. How can you accomplish this transit flow?

● Create a VPC Peering connection between VPC A and VPC B. Create another VPC peering connection between VPC Band VPCC
✓ Create a VPC Peering connection between VPC A and VPC B. Create a VPN connection between VPC B and VPC

● Create a VPC Peering connection between VPC A and VPC C. Create another VPC peering connection between VPC B and VPC C
● Create a VPC Peering connection between VPC A and VPC C. Create a VPN connection between VPC A and VPC

Q37)

Your company currently has a VPC hosted in AWS. There is a private hosted zone in place for the instances in this VPC.

You need your On-premise servers to be able to resolve DNS requests for Instances in the VPC. You need to do this with the least amount of effort.

What steps would you. Choose 2 answers from the options given below.

● Make your On-premise servers point to the new Domain Controller
● Setup an Active Directory Domain Controller in the AWS VPC
✓ Make your On-premise servers point to the Simple AD Instance
✓ Setup a Simple AD Instance in AWS.

Q38)

You are setting up a VPN software on an EC2 Instance which will be used for VPN connections.

Which of the following Is an important aspect that should be set on the EC2 Instance?

● Enable enhanced networking mode on the Amazon EC2 instance.
✓ Disable source destination check on the Amazon EC2 instance
● Enable source destination check on the Amazon EC2 instance.
● Enable route propagation in a Virtual Private Cloud (VPC) subnet route table.

Q39)

Your planning on setting up a VPC with Subnets. The EC2 Instances hosted in the VPC needs to get the time from a custom NTP server.

How can you accomplish this?

● Use an Application Load Balancer and then provide the NW server as part of the ALB configuration.
● Assign the NTP server in the Subnet configuration
✓ Create a DHCP Options set and provide the NTP server name
● Define a resource record in Route 53 and provide the NTP server name

Q40)

You need to have a managed threat detection service that continuously monitors for malicious or unauthorized behavior against your EC2 Instances.

Which of the following can help in such a requirement?

● Amazon VPC Flow Logs
✓ Amazon Guard Duty
● Amazon Cloud Trail
● Amazon Cloud watch Logs

Q41)

There is a requirement to see all port scans which are occurring on a couple of EC2 instances.

Which of the following can be used for such a requirement?

● AWS Cloud watch Events
● AWS Trusted Advisor
✓ AWS VPC Flow Logs
● AWS Inspector

Q42)

Your company has setup a Classic Load Balancer with EC2 Instances behind them. These EC2 Instances are spun up via an Auto scaling group.

In your company there is normally a spike in traffic in the beginning and end of the day. The ELB and Auto scaling Groups have been created with the default settings.

It has been noticed that there are timeouts or partially rendered pages at times. How can this be resolved?

● Change the maximum number of instances setting in the Auto scaling Group
● Enable Cross Zone Load Balancing
✓ Change the Connection Draining timeout in the ELB
● Add another Auto scaling group to the ELB

Q43) Robert is system administrator at TPT Limited and has a VPN connection between on-premise and an AWS VPC. Robert is responsible to ensure instances in the VPC reach the Internet and for which an Internet gateway has been attached. How route tables be configured by Robert so that traffic can flow through the VPN and the Internet?

● None of these
● Setup 2 Route tables. One route table with a default route to the Internet and another one with the s prefix route to the Virtual Private gateway. Attach the Route tables to the subnets in the VPC.
✓ Setup one route table. Add one route of 0.0.0.0/0 to the Internet and one specific prefix route for the Virtual Private gateway. Attach the Route table to the subnets in the VPC.
● Setup 2 Route tables. One route table with a default route to the Internet and another one with the default route to the Virtual Private gateway. Attach the Route tables to the sub nets In the VPC.
● Setup one route table. Add one route of 0.0.0.0/0 to the Internet and another route of 0.0.0.0/0 route for the Virtual Private gateway. Attach the Route table to the subnets In the VPC.

Q44) Robert is IT Manager at TPT Limited and has configured a hosted zone in Route 53. How will Robert be able to see the types of records being requested to the zone?

● None of these
✓ Configure Amazon Route 53 logging
● Configure Cloud watch metrics
● Configure VPC Flow Logs
● Configure Cloud trail

Q45) TPT Limited wants to set up an AWS Direct Connect connection along with a private virtual interface. TPT Limited has 169 IP prefixes to be advertised via the private virtual interface. TPT Limited has made the request and made sure the equipment are in place. Which implementation step will ensure the connection works as per the requirement?

● None of these
✓ Summarize the routes into a default route
● Ensure to also create a public VIF to access the resources in the VPC
● Ensure a VPC Peering connection is in place
● Create a VPN connection

Q46)

You are planning on setting up an AWS VPN managed connection. You have a customer gateway that is behind a NAT device.

In such a case what steps should be taken to ensure proper connectivity. Choose 2 answers from the options given below?

● Ensure the on-premise firewall has TCP port 4500 unblocked
✓ Ensure the on-premise firewall has UDP port 4500 unblocked
✓ Use the public IP address of the NAT device
● Use the private IP address of the customer gateway

Q47) TPT Limited wants to set up an AWS Direct Connect connection to an AWS VPC. How will TPT Limited achieve maximum fault tolerance together with maximum bandwidth at all times?

● None of these
✓ One Virtual Private gateway Two AWS Direct Connect Locations Two Customer gateways
● One Virtual Private gateway One AWS Direct Connect Location One VPN connection
● Two Virtual Private gateway Two AWS Direct Connect Locations One Customer gateway
● Two Virtual Private gateway One AWS Direct Connect Location One Customer gateway

Q48)

Your company is planning on setting up a Direct Connect connection to AWS.

But they don't require or have the facility to accommodate a 1 Gbps connection.

How can they achieve a sub 1 G connection? Choose 2 answers from the options given below.

● If they have a parent AWS Account which can accommodate a 1 G connection, look at having a Hosted Connection
✓ If they have a parent AWS Account which can accommodate a 1 G connection. look at having a Hosted Virtual Interface
● They can consider contacting an AWS Partner for a Hosted Virtual Interface
✓ They can consider contacting an AWS Partner for a Hosted Connection

Q49) TPT Limited is planning to connect their on-premise location to an AWS VPC. Robert has been asked to suggest a solution to meet the following requirements -
1. Configure on-premise servers to resolve custom DNS domain names in the VPC
2. Instances in the VPC to resolve the DNS names of the on-premise servers.

Which of the following solution should Robert suggest in this case?

● None of these
● Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the On-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location
✓ Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Amazon DNS resolver for the VPC. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder, Configure a DNS forwarder in the On-premise location.
● Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Name server for the Route 53 hosted zone. Also ensure the forwarder is configured with the on-premise DNS server, Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a

DNS forwarder in the On-premise location

● Setup a DNS forwarder In your VPC. Ensure the DNS forwarder points to the IP address of the VPN tunnel. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location

Q50) TPT Limited has multiple remote branch offices which are to be connected with AWS VPC. Which of the following will accomplish the task easily?

● VPC Peering
● AWS Direct Connect with a Public V1F
● AWS Direct Connect with a Private VIF
✓ VPN Cloud hub
● None of these

Q51) TPT Limited has just configured a private hosted zone in Route 53 and a VPN connection between the AWS VPC and on-premise network. Which of the following will resolve DNS names from on-premise to the resources records defined in the Private hosted zone?

● None of these
● Create a DNS resolver server in your on-premise location. Configure the VPC with a new DHCP options set which uses this DNS resolver.
✓ Configure a DNS forwarder In the VPC which will forward DNS requests to the Route 53 private hosted zone
● Configure a DNS resolver in the VPC which will resolve DNS requests to the Route 53 private hosted zone.
● Create a DNS forwarder server in your on-premise location. Configure the VPC with a new DHCP options s which uses this DNS forwarder.

Q52)

Your company is planning on using AWS EC2 and ELB for deployment for their web applications.

The security policy mandates that all traffic should be encrypted.

Which of the following options will ensure that this requirement is met. Choose 2 answers from the options below.

✓ Ensure the load balancer listens on port 443
✓ Ensure the HTTPS listener sends requests to the instances on port 443
● Ensure the hTTPS listener sends requests to the Instances on port 80
● Ensure the load balancer listens on port 80

Q53) TPT Limited wants to create a VPC endpoint for their SaaS product hosted in AWS. TPT Limited wants give this link to their customer who will access from their application working on UDP. TPT Limited is planning to provide a DNS name for the link to the customer but, customer complains of not being able to use the link from within their application. Identify the reason for this behaviour.

● The customer needs to create a Network load balancer to access the endpoint service
✓ The service endpoint only works on the TCP protocol
● The customer needs to use a NAT device to access the endpoint service
● The gateway endpoint has a policy that denies access. This should be modified accordingly.
● None of these

Q54) TPT Limited is hosting an application of a NGINX web server which is hosted behind a load balancer. How would TPT Limited ensure restricted access to certain locations for the content hosted on the Web server?

● None of these
● Use the NGINX logs to get the web server variable and then use the IP address to restrict content via Cloud front geo-restrictions.
● Use the ELB logs to create a blacklist for restrictions
● Use the ELB itself to restrict content via geo-restrictions
✓ Use the IP addresses in the X-Forwarded-For HTTP header and then restrict content via Cloud front geo-restrictions.

Q55) TPT Limited is using the Net Flow software for monitoring and accessing details of traffic flows between systems in their On-premise network. Which of the following will provide the same functionality if TPT Limited migrates to AWS?

● AWS Cloudwatch metrics
● AWS Config
● AWS Cloudwatch logs
✓ AWS VPC Flow Logs
● None of these

Q56)

TPT Limited wants to set up an AWS Direct Connect connection to an AWS VPC.

How will TPT Limited achieve maximum fault tolerance together with maximum bandwidth at all times?

● Two Virtual Private gateway One AWS Direct Connect Location One Customer gateway
● Two Virtual Private gateway Two AWS Direct Connect Locations One Customer gateway
● One Virtual Private gateway One AWS Direct Connect Location One VPN connection
✓ One Virtual Private gateway Two AWS Direct Connect Locations Two Customer gateways
● None of these

Q57) TPT Limited is planning to connect their on-premise location to an AWS VPC. Robert has been asked to suggest a solution to meet the following requirements -
1. Configure on-premise servers to resolve custom DNS domain names in the VPC
2. Instances in the VPC to resolve the DNS names of the on-premise servers.

Which of the following solution should Robert suggest in this case?

● Setup a DNS forwarder In your VPC. Ensure the DNS forwarder points to the IP address of the VPN tunnel. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location
● Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Name server for the Route 53 hosted zone. Also ensure the forwarder is configured with the on-premise DNS server, Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location
✓ Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the Amazon DNS resolver for the VPC. Also ensure the forwarder is configured with the on-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder, Configure a DNS forwarder in the On-premise location.
● Setup a DNS forwarder in your VPC. Ensure the DNS forwarder points to the IP address of the On-premise DNS server. Change the Option Set for the VPC for the IP address of the DNS forwarder. Configure a DNS forwarder in the On-premise location
● None of these

Q58)

An IP address range of 11.11.0.0/16 is there in your on-premises network. Only IPs within this network rangecan be used for inter-server communication.

For the cloud the IP address range 11.11.253.0/24 has been allocated.

Now a VPC in AWS needs to be designed. The servers within the VPC should be able to communicate with hostsboth on the Internet and on-premises through a VPN connection.

Your needs are met by what combination of configuration steps?

1.) Set up the VPC with an IP address range of 11.11.253.0/24.

2.) Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set up a NAT gateway to do translation between 10.10.10.0/24 and 11.11.253.0/24 for all outbound traffic.

3.) traffic to the Internet.

4.) Set up a VPN connection between a VGW and an on-premises router, set the VGW as the default gateway for traffic destined to 11.11.0.0/24, and add a VPC subnet route to point the default gateway to an Internet gateway for Internet traffic.

5.) Set up the VPC with an RFC 1918 private IP address range (e.g., 10.10.10.0/24), and set the VGW to do a source IP translation of all outbound packets to 11.11.0.0/16.

● Only 4 and 5
✓ Only 1 and 3
● Only 2, 4 and 5
● Only 1, 3 and 4

Q59)

Riley's application server instances reside in the private subnet of your VPC. These instances need to access a Git repository on the Internet. In the public subnet of your VPC he created a NAT gateway. The NAT gateway can reach the Git repository, while the instances in the private subnet cannot. A default route in the private subnet route table points to the NAT gateway is confirmed by Riley. The security group for his application server instances permits all traffic to the NAT gateway.

To ensure that these instances can reach the patch server what configuration change should be made by Riley?

● Configure an inbound rule on the application server instance security group for the Git repository.
● Configure inbound network access control lists (network ACLs) to allow traffic from the Git repository to the public subnet.
✓ Configure an outbound rule on the application server instance security group for the Git repository.
● Assign public IP addresses to the instances and route 0.0.0.0/0 to the Internet gateway.

Q60)

In an ap-southeast-1 Direct Connect location an AWS Direct Connect connection has been installed by Ted's company. Through a router a public virtual interface is configured to a dedicated firewall. He advertises his company's public /24 CIDR block to AWS with AS 65500. To map all outbound traffic to a single IP the company maintains a separate, corporate Internet firewall. This firewall maintains a BGP relationship with an upstream Internet provider that has delegated the public IP block your company uses. When the BGP session for the public virtual interface is up, corporate network users cannot access Amazon S3 resources in the ap-southeast-1 region.

To provide concurrent AWS and Internet access which step should Ted take?

✓ NAT the traffic destined for AWS from the dedicated firewall using the public virtual interface
● Advertise a host route for the corporate firewall to the upstream Internet provider.
● Advertise a host route for the corporate firewall on the public virtual interface.
● Configure AS-PATH prepending for the public virtual interface.

Q61)

A request to allow S3 access from inside the corporate network Ted's customer's internal security teams receives requests. All external traffic must be explicitly whitelisted through his corporate firewalls.

How this access can be granted by Ted's security team?

● Connect your data center to a VPC via Direct Connect. Create routes that forward traffic from your data center to an S3 private endpoint.
● Obtain the list of IP prefixes by performing a DNS lookup on Amazon S3 endpoints, and use those prefixes in firewall rules.
✓ Obtain the list of IP prefixes from ip-ranges.json, and use those prefixes in firewall rules.
● Obtain the list of IP prefixes from AWS Forum announcements, and use those prefixes in firewall rules.

Q62)

A VPC with the CIDR block of 192.168.0.0./16, was earlier created by the Production team of Ryan. Instances were launched in the VPC. Now there is a decision to ensure the instances have an address space for 10.0.0.0/16.

State the way to achieve this.

● Launch a NAT Instance. Ensure that the instance performs Network address translation onto the CIDR range of 10.0.0.0/16
● Change the address block of the VPC from 192.168.0.0./16 to 10.0.0.0/16. All of the instances will now use the new address space.
✓ Create a new VPC with the address block of 10.0.0.0/16. Migrate all of the instances to the new VPC.
● Add a new address space to the VPC. Then ensure that the instances use the new address space

Q63)

"Nick's architecture team has recommended the following for the VPC's in his AWS Account.

A shared services VPC which would provide services to other VPC's.

A hosted VPC that will be accessible to the customer. The hosted VPC will also interact with the shared services VPC. Considering the following options, select the which should be Considered as a Part of the design.

1.) Ensure a virtual private link is available for accessing the Shared services VPC

2.) Use VPC peering between the shared services VPC and other VPC's

3.) Put the shared services VPC as public. Ensure the right security measures are in place for accessing the shared services.

4.) Create a VPN between each VPC. Ensure the Virtual private gateway is in place for the other VPC's

● Only 1 and 2
● Only 2 and 4
● Only 3 and 4
✓ Only 1 and 3

Q64)

Ryan VPC consists of public and private subnets. The private subnets make use of a NAT instance to download updates from the internet.

The Instances are trying to download updates from a server which listens on port 8090.

But the instances are not able to reach the external server for updates.

Out of the following options, select the Relevant issues with this.

1.) The NAT instance is blocking traffic on port 8090

2.) The Inbound NACL is blocking traffic on port 8090

3.) The Inbound Security Groups are blocking traffic on port 8090

4.)The remote server firewall is blocking traffic

● Only 2 and 4
● Only 1 and 3
Explanation:-The NAT instance could be blocking Outbound Traffic on port 8090 which is not allowing traffic to flow outwards. The remote server could also be blocking traffic from the instances. Options B and C are invalid because the traffic is Outbound on port 8090 and not Inbound on port 8090.
✓ Only 1 and 4
● Only 3 and 4

Q65)

"In a Private subnet Nessy's company has a set of instances hosted.

These instances need to make calls to the Simple Storage Service.

She has setup the Endpoint but are still not able to access the S3 buckets from the instances in the Private subnet.

Out of the following select which could be issues for the access'

1.) You should be using an interface instead of a gateway for accessing the S3 service.

2.) The prefix for the endpoint is not attached to the Route table

3.) The prefix for the endpoint is not attached to the Security Group

4.)Bucket policy attached to S3 buckets doesn't allow access to VPC endpoint

● Only 1 and 2
✓ Only 2 and 4
● Only 3 and 4
● Only 1