Free Questions for ACE by dumpssheet

Shared by Nichols on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are the connectivity options for customers to access Azure?

Options:

A- Internet Only

B- VPN and Express Route

C- Internet, VPN, and DirectConnect

D- Internet, VPN, ExpressRoute

Answer:

D

Explanation:

Basically, there are 4 options for consumers to access Azure:

* Internet connectivity.

* Point-to-site VPN (P2S VPN)

* Site-to-Site VPN (S2S VPN)

* ExpressRoute.

Question 2

Question Type: **MultipleChoice**

Can the Aviatrix platform help you interconnect VPCs/VNets/VCNs with overlapping IP address ranges?

Options:

A- Yes, using standard encrypted peering

B- Yes, using S2C (Site-to-Cloud)

C- Yes, using FiightPath

D- No

Answer:

B

Explanation:

Site2Cloud builds an encrypted connection between two sites over the Internet, in an easy to

use and template driven manner. Its workflow is similar to AWS VGW or Azure VPN.

Overlapping IP addresses The CIDR blocks at your customer sites are not controlled by us. If CIDR

block overlaps with our operation VPC CIDR, we have to find a way to NAT the address. The cloud

provider native solution is not usable in this case. The Aviatrix site2cloud solution solves this problems:

Question 3

Question Type: DragDrop

Match the terminology to the appropriate Public Cloud provider.

Answer:

Question 4

Question Type: MultipleChoice

ACE Inc. has a VNet-A hosting Database services which is peered with several app VNets. There is a new requirement to add another CIDR to VNet-

Options:

A- How can you prevent a database connectivity outage for all the peered VNets while performing this task?

A- Use powershell to update the VNet-A CIDR

B- You cannot add a CIDR to a VNet after It has been created

C- It's not possible to perform this action without an outage as you need to delete all existing peering before new CIDR can be added

D- First modify peering routes for all the VNets to add the new CIDR and then add the new CIDR to VNET-A

Answer:

D

Question 5

Question Type: MultipleChoice

ACE Inc. is currently using AWS Transit Gateway (TGW) with 100 VPCs attached to it from different security domains.

These 100 VPCs are used as following:

* 20 VPCs belong to Production,

* 40 VPCs belong to Development,

* 20 are part of UAT and

* 20 VPCs are for shared services and miscellanous common needs.

ACE Inc. requirements are to:

* provide network and traffic segmentation between Prod, Development, UAT VPCs such that there is no traffic between VPCs belonging to different domains

* allow all VPCs in each domain to communicate with each other

* allow every VPC access to shared services VPCs

Which Aviatrix feature would help to not only provide this segmentation but also decrease the complexity of this topology and routing configuration by orchestrating life-cycle management of AWS Transit Gateways?

(Choose 2)

Options:

A- Aviatrix AWS-TGW Encrypted Peering

B- Aviatrix TGW Orchestrator

C- Aviatrix Security Domain

D- Aviatrix Slte-io-Cloud (S2C)

Answer:

B, C

Explanation:

A Security Domain is an enforced network of member VPCs attached to the same route table. Member VPCs

have connectivity to each other. VPCs outside of the domain cannot connect. A Security Domain is an

instantiation of the AWS Transit Gateway (TGW) Route Domain concept. This enables VPC segmentation

through AWS Transit Gateway (TGW). For example, you can have "dev", "prod" and "test" security domains toisolate your development, production and test environments in your AWS cloud. In this scenario, the VPCs in dev security domain cannot talk to VPCs in prod and test security domains. A security domain can have one or more spoke VPCs as its members. VPCs within a security domain can communicate to each other via AWS Transit

Gateway (TGW).

we can leverage domains with the AWS Transit Gateway to segment and secure your network.

The AWS Transit Gateway (TGW) Orchestrator is a feature in Aviatrix Controller. It provides a point-andclick workflow to build a transit network and manages all network routing updates.

Aviatrix orchestrator (available in the AVX Controller) simplifies and extends the AWS Transit Gateway (TGW)

by using dynamic route propagation, policy abstraction and simplifying operations through a single pane of glass.

Question 6

Question Type: **MultipleChoice**

What is/are the protocol(s) supported by Aviatrix Site2Cloud (S2C) Gateway?

Options:

A- GRE

B- UDP only

C- Both TCP and UDP

D- TCP only

Answer:

C

Question 7

Question Type: **MultipleChoice**

High speed private connectivity from customer locations (data centers, Headquarters) to public cloud such as AWS Direct Connect, Azure ExpressRoute, Google Interconnect and OCI FastConnect are encrypted by default?

Options:

A- Ture

B- False

Answer:

B

Explanation:

AWS Direct Connect is a private link into AWS regions that provides bandwidth. The service

is not natively encrypted when initially deployed.

Express Route does not provide network traffic encryption for its circuits!

Google InterConnect NOT encrypted by default.

Question 8

Question Type: MultipleChoice

Which networking entity in the cloud infrastructure allows operators to run commands to see BGP state, route tables, diagnostic, logs etc.

Options:

A- AWSVPC Implicit Router

B- Azure VNET Router

C- Google Cloud Router

D- Aviatrix Gateway

Answer:

D

Question 9

Question Type: MultipleChoice

What is a challenge of using ExpressRoute Edge Routers as transit to interconnect VNets in Azure?

Options:

A- Not recommended by Microsoft Product Group / not officially documented

B- BW limited by ExpressRoute Gateway SKU

C- Limited Control of routing propagation

D- All of the above

Answer:

D

Question 10

Question Type: MultipleChoice

ACE Inc. had been using a standard marketplace router as an NVA (Network Virtual Appliance) in the hub Virtual Network (VNet) for spoke to spoke communication. The NVA has just been replaced by Azure Firewall.

Now the security operations team is reporting that traffic between Virtual Machines in the same VNet is working however any inter-VNet traffic is being dropped by the NSGs (Network Security Groups) at destination.

What could be a possible reason?

Options:

A- Azure Firewall is blocking all the traffic

B- There is no route at the Azure Firewall

C- Azure Firewall is doing SNAT for inter-VNet traffic

D- BGP routes in UDR need to be updated

Answer:

C

Explanation:

Azure Firewall provides automatic SNAT for all outbound traffic to public IP addresses. By default, Azure Firewall doesn't SNAT with Network rules when the destination IP address is in a private IP address range per IANA RFC 1918. Application rules are always applied using a transparent proxy regardless of the destination IP address.

This logic works well when you route traffic directly to the Internet. However, if you've enabled forced tunneling, Internet-bound traffic is SNATed to one of the firewall private IP addresses in

AzureFirewallSubnet, hiding the source from your on-premises firewall.

If your organization uses a public IP address range for private networks, Azure Firewall SNATs the traffic to one of the firewall private IP addresses in AzureFirewallSubnet. However, you can configure Azure Firewall to not SNAT your public IP address range.

To configure Azure Firewall to never SNAT regardless of the destination IP address, use 0.0.0.0/0 as your private IP address range. With this configuration, Azure Firewall can never route traffic directly to theInternet. To configure the firewall to always SNAT regardless of the destination address, use 255.255.255.255/32 as your private IP address range.

Question 11

Question Type: MultipleChoice

Choose the best definition for Firewall Network (FireNet)?

Options:

A- Aviatrix turn key solution to scalably deploy firewall instances in the cloud

B- Azure functionality to deploy 3rd party firewalls in a VPC

C- AWS functionality to deploy 3rd party firewalls in a VPC

D- GCP functionality to deploy 3rd party firewalls in a VPC

Answer:

A

Explanation:

Firewall Network (FireNet) Workflow Aviatrix Firewall Network (FireNet) is a turn key network solution to deploy firewall instances in the cloud.

FireNet is a solution for integrating firewalls in the AWS TGW deployment.

Question 12

Question Type: MultipleChoice

An example of when would you use Aviatrix FlightPath is:

Options:

A- To insert Firewall into traffic path between 2 VPCs

B- To connect your branch office to the cloud resources

C- To view controller logs

D- To troubleshoot connectivity between EC2 instances in 2 AWS VPCs

Answer:

D

Explanation:

EC2 related information such as Security Groups, Route table and route table entries and network ACL.

This helps you to identify connectivity problems.

You do not need to launch Aviatrix gateways to use this tool, but you need to create Aviatrix accounts so

that the Controller can use the account credentials to execute AWS APIs to retrieve relevant information.