Free Questions for NSE7_PBC-7.2 by go4braindumps

Shared by Bass on 24-10-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to deploy FortiGate VM devices in a highly available topology in the Microsoft Azure cloud. The following are the requirements of your deployment:

* Two FortiGate devices must be deployed; each in a different availability zone.

* Each FortiGate requires two virtual network interfaces: one will connect to a public subnet and the other will connect to a private subnet.

* An external Microsoft Azure load balancer will distribute ingress traffic to both FortiGate devices in an active- active topology.

* An internal Microsoft Azure load balancer will distribute egress traffic from protected virtual machines to both FortiGate devices in an active-active topology.

* Traffic should be accepted or denied by a firewall policy in the same way by either FortiGate device in this topology.

Which FortiOS CLI configuration can help reduce the administrative effort required to maintain the FortiGate devices, by synchronizing firewall policy and object configuration between the FortiGate devices?

Options:

A- config system sdn-connector

B- config system ha

C- config system auto-scale

D- config system session-sync

Answer:

B

Explanation:

FTG HA Active/Active requires the following configuration to sync the session by FGSP

config system ha

set session-pickup enable

set session-pickup-connectionless enable

set session-pickup-nat enable

set session-pickup-expectation enable

set override disable

end

config system cluster-sync

edit 0

set peerip 10.0.1.x

set syncvd 'root'

next

end

https://github.com/fortinet/azure-templates/tree/main/FortiGate/Active-Active-ELB-ILB

Question 2

Question Type: **MultipleChoice**

Customer XYZ has an ExpressRoute connection from Microsoft Azure to a data center. They want to secure communication over ExpressRoute, and to install an in-line FortiGate to perform intrusion prevention system (IPS) and antivirus scanning.

Which three methods can the customer use to ensure that all traffic from the data center is sent through FortiGate over ExpressRoute? (Choose three.)

Options:

A- Install FortiGate in Azure and build a VPN tunnel to the data center over ExpressRoute

B- Configure a user-defined route table

C- Enable the redirect option in ExpressRoute to send data center traffic to a user-defined route table

D- Configure the gateway subnet as the subnet in the user-defined route table

E- Define a default route where the next hop IP is the FortiGate WAN interface

Answer:

A, D, E

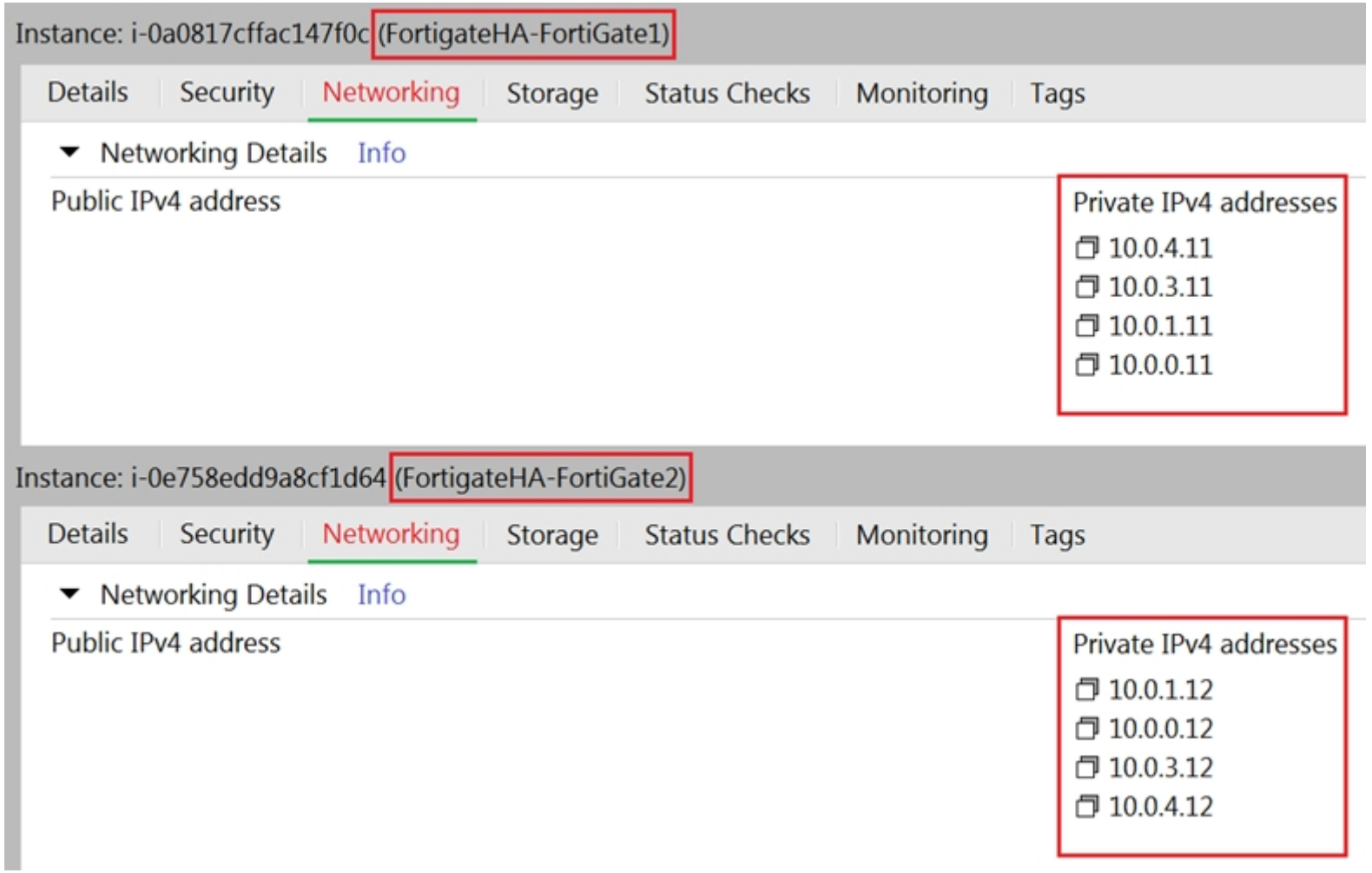
Explanation:

https://docs.microsoft.com/en-us/answers/questions/618005/adding-a-inline-fw-to-express-route.html

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



You are configuring an active-passive FortiGate clustering protocol (FGCP) HA configuration in a single availability zone in Amazon Web Services (AWS), using a cloud formation template.

After deploying the template, you notice that the AWS console has IP information listed in the FortiGate VM firewalls in the HA configuration. However, within the configuration of FortiOS, you notice that port1 is using an IP of 10.0.0.13, and port2 is using an IP of 10.0.1.13.

What should you do to correct this issue?

Options:

A- Configure FortiOS to use static IP addresses with the IP addresses reflected in the ENI primary IP address configuration (as per the exhibit).

B- Delete the deployment and start again. You have in put the wrong parameters during the cloud formation template deployment.

C- Configure FortiOS to use DHCP so that it will get the correct IP addresses on the ports.

D- Nothing, in AWS cloud, it is normal for a FortiGate ENI primary IP address to be different than the FortiOS IP address configuration.

Answer:

D

Question 4

Question Type: **MultipleChoice**

Which statement about FortiSandbox in Amazon Web Services (AWS) is true?

Options:

A- In AWS, virtual machines (VMs) that inspect files do not have to be reset after inspecting a file.

B- FortiSandbox in AWS uses Windows virtual machines (VMs) to inspect files.

C- In AWS, virtual machines (VMs) that inspect files are constantly up and running.

D- FortiSandbox in AWS can have a maximum of eight virtual machines (VMs) that inspect files.

Answer:

B

Explanation:

FortiSandbox deploys new EC2 instances with the custom Windows VMs, and then it sends malware, runs it, and captures the results for analysis. FortiSandbox for AWS does not need more resources because it performs management and analysis tasks only. Note that the cost varies based on the number of EC2 instances deployed, size of the instances, and duration of the running time.

Question 5

Question Type: MultipleChoice

You have been asked to develop an Azure Resource Manager infrastructure as a code template for the FortiGate-VM, that can be reused for multiple deployments. The deployment fails, and errors point to the storageAccount name.

Which two are restrictions for a storageAccount name in an Azure Resource Manager template? (Choose two.)

Options:

A- The uniqueString() function must be used.

B- The storageAccount name must use special characters.

C- The storageAccount name must be in lowercase.

D- The storageAccount name must contain between 3 and 24 alphanumeric characters.

Answer:

C, D

Explanation:

-Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.
https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview

https://docs.microsoft.com/en-us/azure/templates/microsoft.storage/storageaccounts?tabs=bicep

Property values / storageAccounts

name --> The resource name :

* string (required)

* Character limit: 3-24

* Valid characters: Lowercase letters and numbers.

* Resource name must be unique across Azure.

Question 6

Question Type: **MultipleChoice**

An organization deployed a FortiGate-VM in the Google Cloud Platform and initially configured it with two vNICs. Now, the same organization wants to add additional vNICs to this existing FortiGate-VM to support different workloads in their environment.

How can they do this?

Options:

A- They can create additional vNICs using the Cloud Shell.

B- They cannot create and add additional vNICs to an existing FortiGate-VM.

C- They can create additional vNICs in the UI console.

D- They can use the Compute Engine API Explorer.

Answer:

B

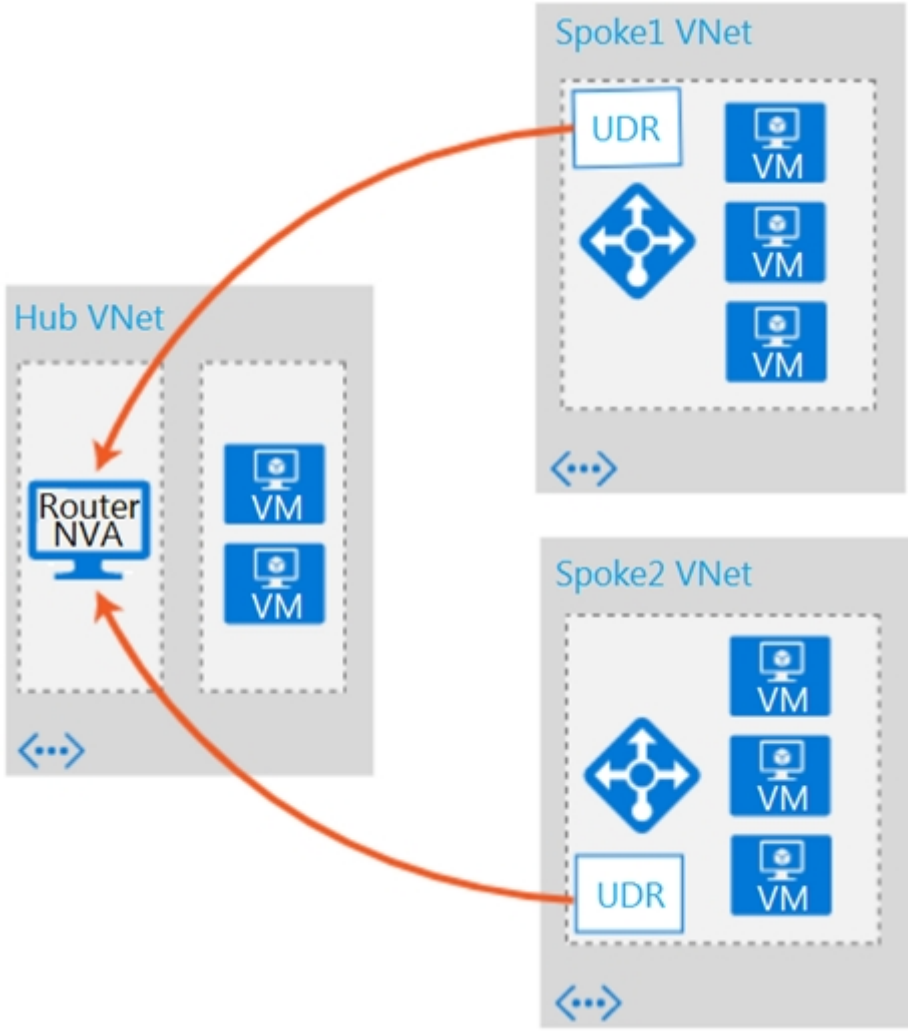
Explanation:

GCP Limitations: You cannot add or remove network interfaces from an existing VM. https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#limitations

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



Which two conditions will enable you to segregate and secure the traffic between the hub and the spokes in Microsoft Azure? (Choose two.)

Options:

A- Implement the FortiGate-VM network virtual appliance (NVA) in the hub and use user-defined routes (UDRs) in the spokes.

B- Use ExpressRoute to interconnect the hub VNets and spoke VNets.

C- Configure VNet peering between the spokes only.

D- Configure VNet peering between the hub and spokes.

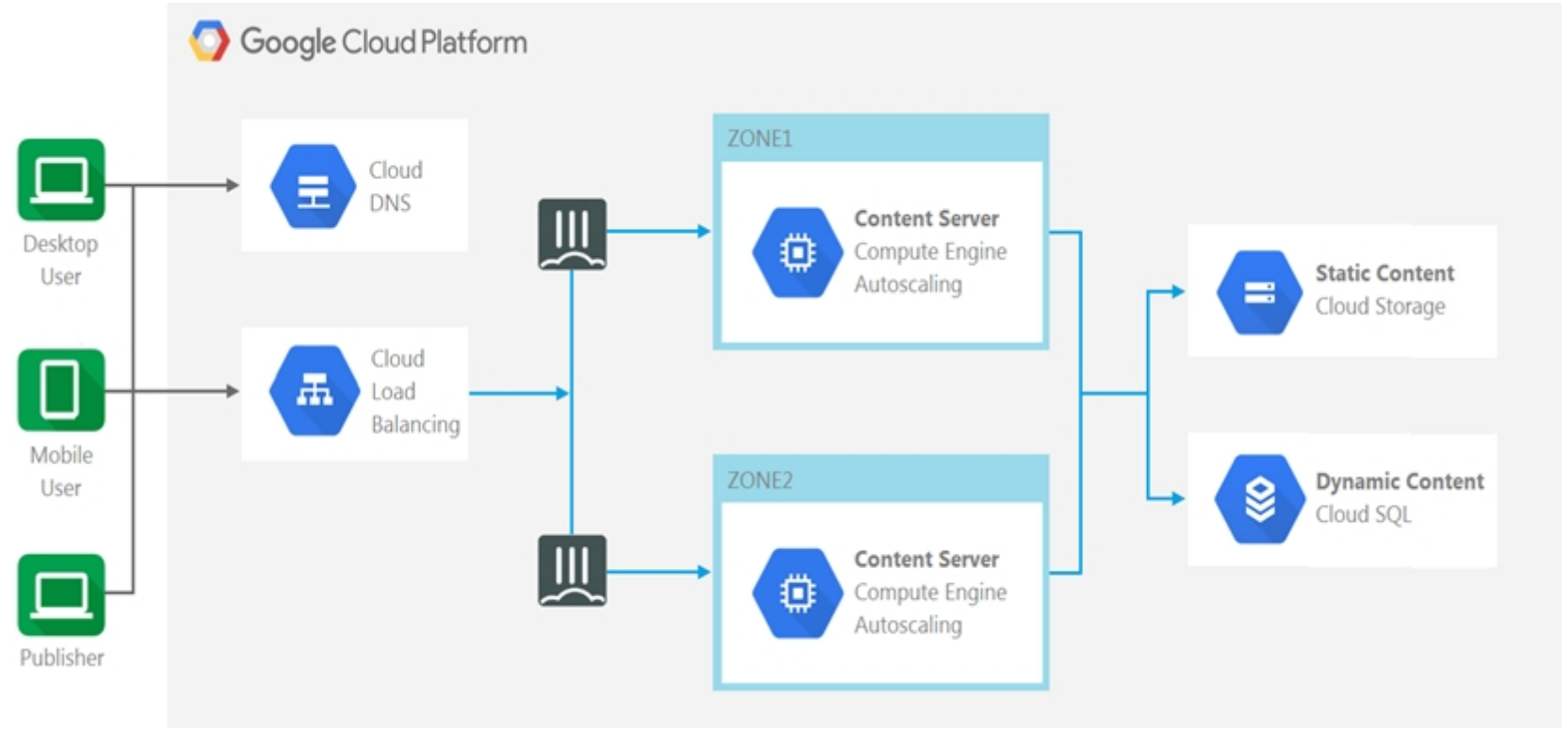
Answer:

A, D

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



The exhibit shows a topology where multiple connections from clients to the same FortiGate-VM instance, regardless of the protocol being used, are required.

Which two statements are correct? (Choose two.)

Options:

A- The design shows an active-active FortiGate-VM architecture.

B- The Cloud Load Balancer Session Affinity setting should be changed to CLIENT_IP.

C- The design shows an active-passive FortiGate-VM architecture.

D- The Cloud Load Balancer Session Affinity setting should use the default value.

Answer:

A, B

Explanation:

https://github.com/fortinet/fortigate-autoscale-gcp/blob/main/network.tf session_affinity = 'CLIENT_IP'

A - we using A-A architecture with GCP NLB

B to ensure that the same client always reach the same machine regardless the protocol we must configure a session affinity that route the same source IP to the same instance

as we can see in the TF deployment file

https://github.com/fortinet/fortigate-autoscale-gcp/blob/main/network.tf

'### Target Pools ###

resource 'google_compute_target_pool' 'default' {

```
name = '${var.cluster_name}-instancepool-${random_string.random_name_post.result}'

session_affinity = 'CLIENT_IP'

health_checks = [

'${google_compute_http_health_check.default.name}',

]

}

'
```

Question 9

Question Type: **MultipleChoice**

An organization deploys a FortiGate-VM (VM04 / c4.xlarge) in Amazon Web Services (AWS) and configures two elastic network interfaces (ENIs). Now, the same organization wants to add additional ENIs to support different workloads in their environment.

Which action can you take to accomplish this?

Options:

A- None, you cannot create and add additional ENIs to an existing FortiGate-VM.

B- Create the ENI, shut down FortiGate, attach the ENI to FortiGate, and then start FortiGate.

C- Create the ENI, attach it to FortiGate, and then restart FortiGate.

D- Create the ENI and attach it to FortiGate.

Answer:

D

Explanation:

https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/aws-administration-guide/903457

AWS says that you can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach). It applies to windows: https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/best-practices-for-configuring-network-interfaces.html

Question 10

Question Type: MultipleChoice

Which two statements about Amazon Web Services (AWS) networking are correct? (Choose two.)

Options:

A- Proxy ARP entries are disregarded.

B- 802.1q VLAN tags are allowed inside the same virtual private cloud.

C- AWS DNS reserves the first host IP address of each subnet.

D- Multicast traffic is not allowed.

Answer:

A, D

Explanation:

https://blog.ipspace.net/2018/05/amazon-web-services-networking-overview.html

Question 11

Question Type: MultipleChoice

You have previously deployed an Amazon Web Services (AWS) transit virtual private cloud (VPC) with a pair of FortiGate firewalls (VM04 / c4.xlarge) as your security perimeter. You are beginning to see high CPU usage on the FortiGate instances.

Which action will fix this issue?

Options:

A- Convert the c4.xlarge instances to m4.xlarge instances.

B- Migrate the transit VPNs to new and larger instances (VM08 / c4.2xlarge).

C- Convert from IPsec tunnels to generic routing encapsulation (GRE) tunnels, for the VPC peering connections.

D- Convert the transit VPC firewalls into an auto-scaling group and launch additional EC2 instances in that group.

Answer:

D

Explanation:

Multiple FortiGate-VM instances form an Auto Scaling group to provide highly efficient clustering at times of high workloads. FortiGate-VM instances can be scaled out automatically according to predefined workload levels. https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/aws-administration-guide/397979/deploying-auto-scaling-on-aws

Question 12

Question Type: MultipleChoice

Which two Amazon Web Services (AWS) topologies support east-west traffic inspection within the AWS cloud

by the FortiGate VM? (Choose two.)

Options:

A- A single VPC deployment with multiple subnets and a NAT gateway

B- A single VPC deployment with multiple subnets

C- A multiple VPC deployment utilizing a transit VPC topology

D- A multiple VPC deployment utilizing a transit gateway

Answer:

C, D

Explanation:

Multi-VPC design. AWS recommends segmenting networks at the VPC level. In this approach, workloads are grouped together at the VPC level instead of the subnet level. All traffic between VPCs will be inspected by network security virtual firewalls at each VPC or at a shared VPC. Design patterns such as Transit VPC or AWS Transit Gateway can be used to achieve this in an automated and scalable fashion.