NSE7_PBC-6.4 Q&As

Fortinet NSE 7 - Public Cloud Security 6.4

Pass Fortinet NSE7_PBC-6.4 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/nse7_pbc-6-4.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet Official Exam Center

QUESTION 1

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?

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.

Correct Answer: D

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/62d32ecf-687f-11ea9384-00505692583a/FortiOS-6.4-GCP_Cookbook.pdf

QUESTION 2

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?

A. config system sdn-connector

B. config system ha

C. config system auto-scale

D. config system session-sync

Correct Answer: B

Reference: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/84777/using-standaloneconfiguration-synchronization

QUESTION 3

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

B. Configure a user-defined route table

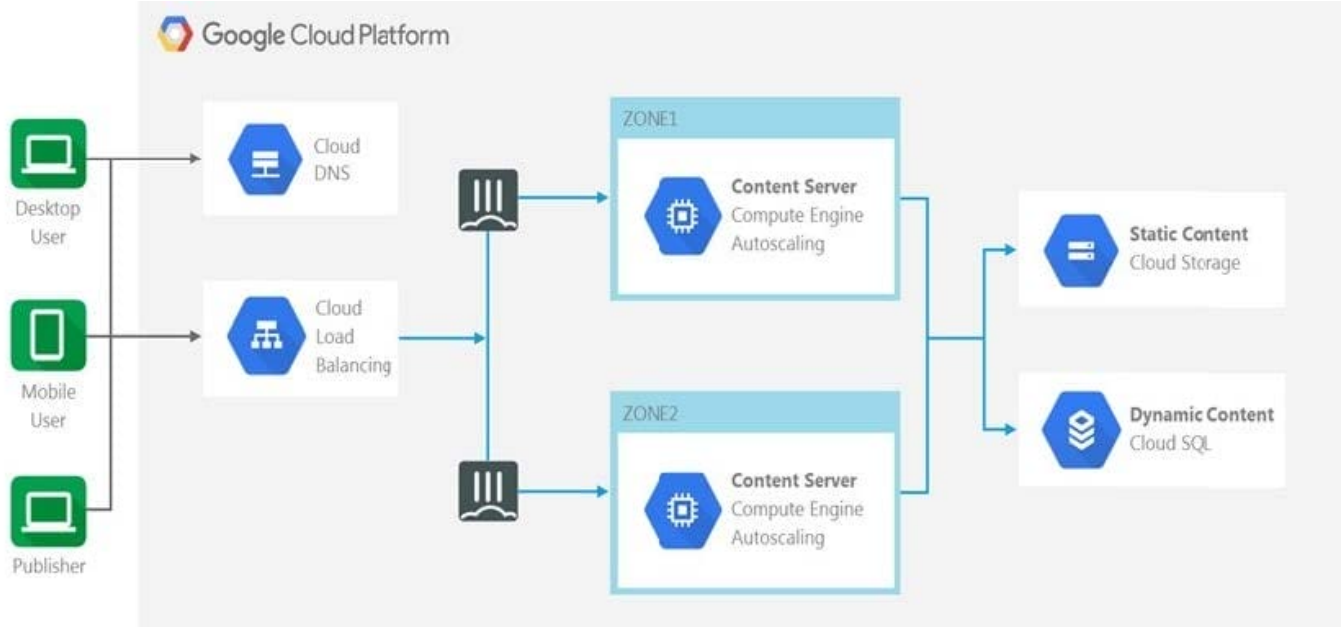
C. Enable the redirect option in ExpressRoute to send data center traffic to a user-defined route table

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

Correct Answer: CDE

QUESTION 4



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.)

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.

Correct Answer: AB

QUESTION 5

You are deploying Amazon Web Services (AWS) GuardDuty to monitor malicious or unauthorized behaviors related to AWS resources. You will also use the Fortinet aws-lambda-guardduty script to translate feeds from AWS GuardDuty findings into a list of malicious IP addresses. FortiGate can then consume this list as an external threat feed.

Which Amazon AWS services must you subscribe to in order to use this feature?

A. GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield.

B. GuardDuty, CloudWatch, S3, and DynamoDB.

C. Inspector, Shield, GuardDuty, S3, and DynamoDB.

D. WAF, Shield, GuardDuty, S3, and DynamoDB.

Correct Answer: A

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424