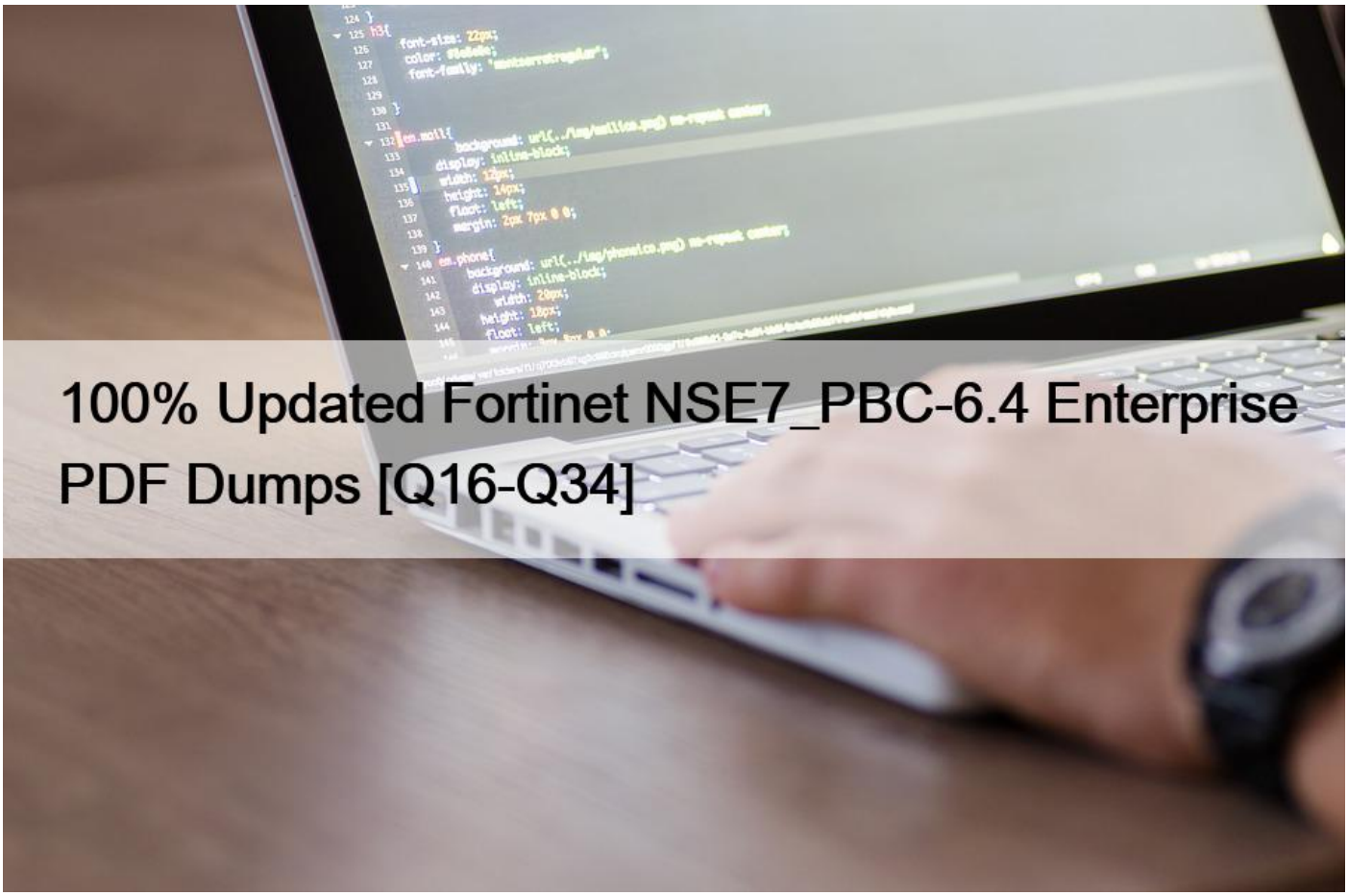
100% Updated Fortinet NSE7_PBC-6.4 Enterprise PDF Dumps [Q16-Q34



100% Updated Fortinet NSE7_PBC-6.4 Enterprise PDF Dumps
Use Valid Exam NSE7_PBC-6.4 by VCEPrep Books For Free Website

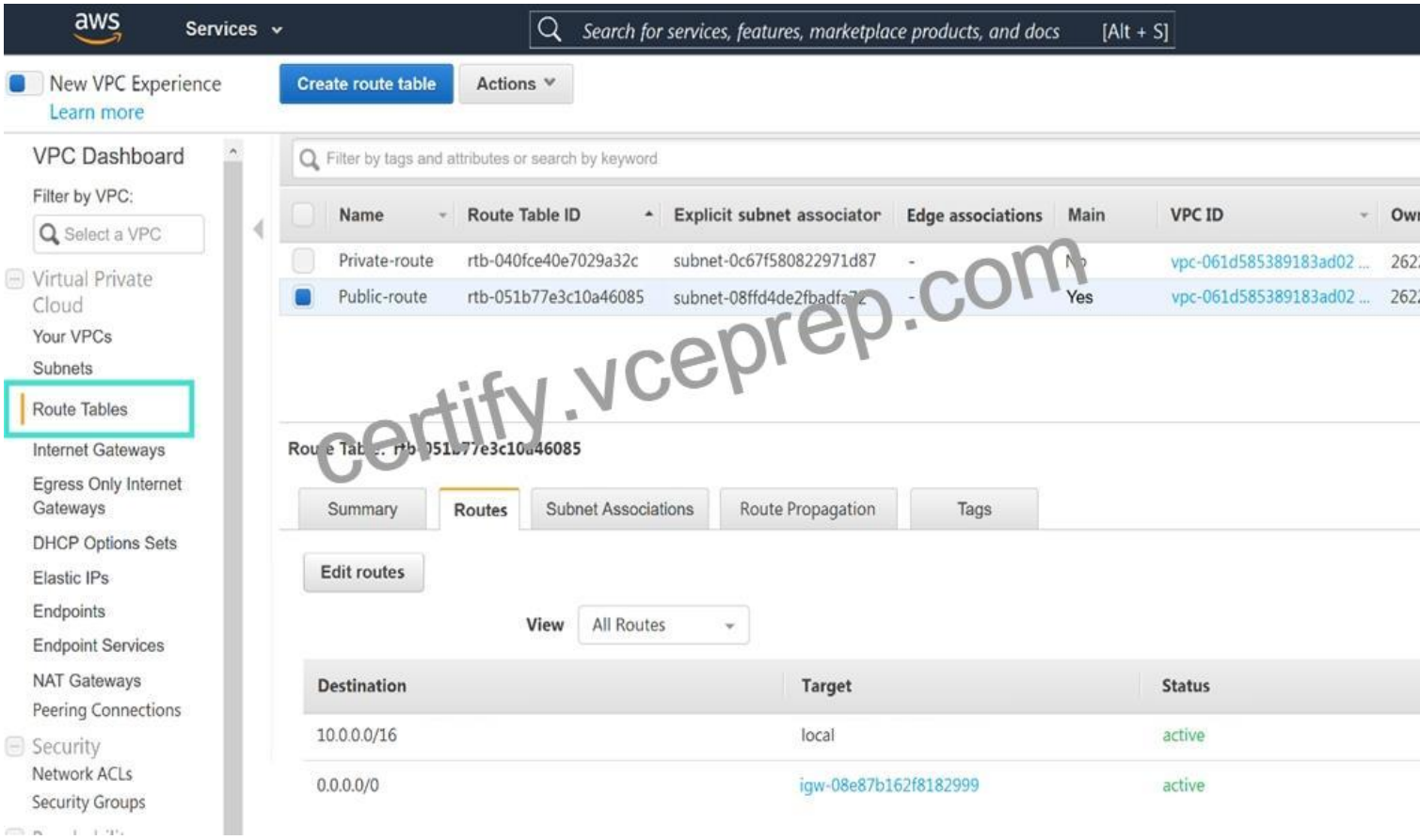
NEW QUESTION 16

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.)
* The uniqueString() function must be used.
* The storageAccount name must use special characters.
* The storageAccount name must be in lowercase.
* The storageAccount name must contain between 3 and 24 alphanumeric characters.

NEW QUESTION 17

Refer to the exhibit.



In your Amazon Web Services (AWS) virtual private cloud (VPC), you must allow outbound access to the internet and upgrade software on an EC2 instance, without using a NAT instance. This specific EC2 instance is running in a private subnet: 10.0.1.0/24.

Also, you must ensure that the EC2 instance source IP address is not exposed to the public internet. There are two subnets in this VPC in the same availability zone, named public (10.0.0.0/24) and private (10.0.1.0/24).

How do you achieve this outcome with minimum configuration?
* Deploy a NAT gateway with an EIP in the private subnet, edit the public main routing table, and change the destination route 0.0.0.0/0 to the target NAT gateway.
* Deploy a NAT gateway with an EIP in the public subnet, edit route tables, select Public-route, and delete the route destination 10.0.0.0/16 to target local.
* Deploy a NAT gateway with an EIP in the private subnet, edit route tables, select Private-route, and add a new route destination 0.0.0.0/0 to the target internet gateway.
* Deploy a NAT gateway with an EIP in the public subnet, edit route tables, select Private-route and add a new route destination 0.0.0.0/0 to target the NAT gateway.

NEW QUESTION 18

You have been tasked with deploying FortiGate VMs in a highly available topology on the Amazon Web Services (AWS) cloud. The requirements for your deployment are as follows:

* You must deploy two FortiGate VMs in a single virtual private cloud (VPC), with an external elastic load balancer which will distribute ingress traffic from the internet to both FortiGate VMs in an active-active topology.

* Each FortiGate VM must have two elastic network interfaces: one will connect to a public subnet and other will connect to a private subnet.

* To maintain high availability, you must deploy the FortiGate VMs in two different availability zones.

How many public and private subnets will you need to configure within the VPC?
* One public subnet and two private subnets
* Two public subnets and one private subnet
* Two public subnets and two private subnets
* One public subnet and one private subnet

NEW QUESTION 19

Your company deploys FortiGate VM devices in high availability (HA) (active-active) mode with Microsoft Azure load balancers using the Microsoft Azure ARM template. Your senior administrator instructs you to connect to one of the FortiGate devices and configure the necessary firewall rules. However, you are not sure now to obtain the correct public IP address of the deployed FortiGate VM and identify the access ports.

How do you obtain the public IP address of the FortiGate VM and identify the correct ports to access the device?
* In the configured load balancer, access the inbound NAT rules section.
* In the configured load balancer, access the backend pools section.
* In the configured load balancer, access the inbound and outbound NAT rules section.
* In the configured load balancer, access the health probes section.

NEW QUESTION 20

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?
* None, you cannot create and add additional ENIs to an existing FortiGate-VM.
* Create the ENI, shut down FortiGate, attach the ENI to FortiGate, and then start FortiGate.
* Create the ENI, attach it to FortiGate, and then restart FortiGate.
* Create the ENI and attach it to FortiGate.

NEW QUESTION 21

What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?
* Up to 1.25 Gbps per attachment
* Up to 50 Gbps per attachment
* Up to 10 Gbps per attachment
* Up to 1 Gbps per attachment

NEW QUESTION 22

Which statement about FortiSandbox in Amazon Web Services (AWS) is true?
* In AWS, virtual machines (VMs) that inspect files do not have to be reset after inspecting a file.
* FortiSandbox in AWS uses Windows virtual machines (VMs) to inspect files.
* In AWS, virtual machines (VMs) that inspect files are constantly up and running.

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

NEW QUESTION 23

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?
* They can create additional vNICs using the Cloud Shell.
* They cannot create and add additional vNICs to an existing FortiGate-VM.
* They can create additional vNICs in the UI console.
* They can use the Compute Engine API Explorer.

NEW QUESTION 24

Which two statements about Microsoft Azure network security groups are true? (Choose two.)
* Network security groups can be applied to subnets and virtual network interfaces.
* Network security groups can be applied to subnets only.
* Network security groups are stateless inbound and outbound rules used for traffic filtering.
* Network security groups are a stateful inbound and outbound rules used for traffic filtering.
Explanation/Reference: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview

NEW QUESTION 25

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?
* config system sdn-connector
* config system ha
* config system auto-scale
* config system session-sync

NEW QUESTION 26

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-guarddutyscript 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?
* GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield.
* GuardDuty, CloudWatch, S3, and DynamoDB.
* Inspector, Shield, GuardDuty, S3, and DynamoDB.
* WAF, Shield, GuardDuty, S3, and DynamoDB.
Explanation/Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424-11e9-

94bf-00505692583a/FortiOS_6.2.0_AWS_Cookbook.pdf

NEW QUESTION 27

What is the bandwidth limitation of an Amazon Web Services (AWS) transit gateway VPC attachment?
* Up to 1.25 Gbps per attachment
* Up to 50 Gbps per attachment
* Up to 10 Gbps per attachment
* Up to 1 Gbps per attachment
Explanation/Reference: https://d1.awsstatic.com/whitepapers/building-a-scalable-and-secure-multi-vpc-aws-network-infrastructure.pdf (5)

NEW QUESTION 28

An Amazon Web Services (AWS) auto-scale FortiGate cluster has just experienced a scale-down event, terminating a FortiGate in availability zone C.

This has now black-holed the private subnet in this availability zone.

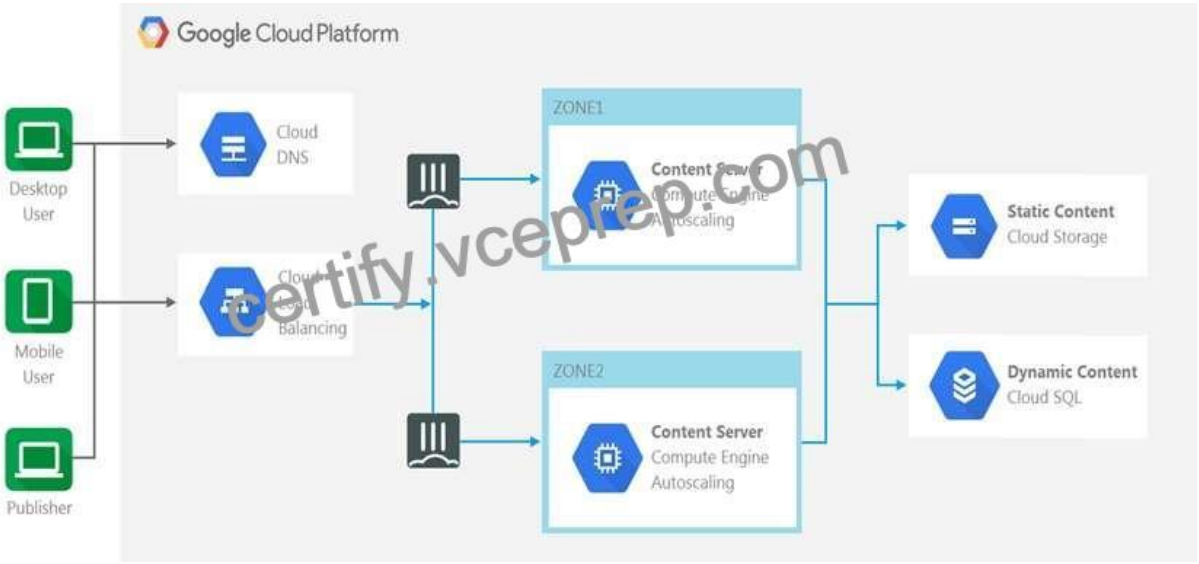
What action will the worker node automatically perform to restore access to the black-holed subnet?
* The worker node applies a route table from a non-black-holed subnet to the black-holed subnet.
* The worker node moves the virtual IP of the terminated FortiGate to a running FortiGate on the worker node’s private subnet interface.
* The worker node modifies the route table applied to the black-holed subnet changing its default route to point to a running FortiGate on the worker node’s private subnet interface.
* The worker node migrates the subnet to a different availability zone.

NEW QUESTION 29

Which two statements about the Amazon Cloud Services (AWS) network access control lists (ACLs) are true?

(Choose two.)
* Network ACLs are stateless, and inbound and outbound rules are used for traffic filtering.
* Network ACLs are stateful, and inbound and outbound rules are used for traffic filtering.
* Network ACLs must be manually applied to virtual network interfaces.
* Network ACLs support allow rules and deny rules.
Explanation/Reference: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NEW QUESTION 30



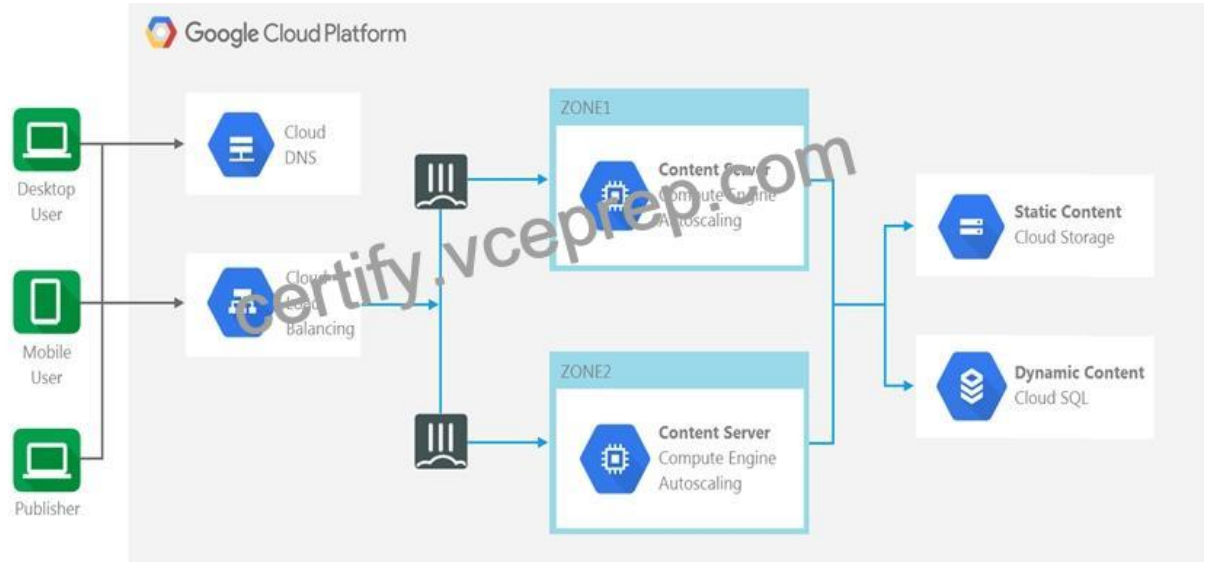
Refer to the exhibit. The exhibit shows a topology where multiple connections from clients to the same FortiGate-VM instance, regardless of the protocol being used, are required.

Which two statements are correct? (Choose two.)

* The design shows an active-active FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should be changed to CLIENT_IP.
* The design shows an active-passive FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should use the default value.

NEW QUESTION 31

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.)
* The design shows an active-active FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should be changed to CLIENT_IP.
* The design shows an active-passive FortiGate-VM architecture.
* The Cloud Load Balancer Session Affinity setting should use the default value.

NEW QUESTION 32

Refer to the exhibit.

You attempted to deploy the FortiGate-VM in Microsoft Azure with the JSON template, and it failed to boot up. The exhibit shows an excerpt from the JSON template.

What is incorrect with the template?
* The LUN ID is not defined.
* FortiGate-VM does not support managedDisk from Azure.
* The caching parameter should be None.
* The CreateOptions parameter should be FromImage.

Fortinet NSE7_PBC-6.4 Official Cert Guide PDF: https://www.vceprep.com/NSE7_PBC-6.4-latest-vce-prep.html]