



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.geekcert.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

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





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 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>

QUESTION 3

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?

- 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.

Correct Answer: B

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/9e3b59dc-ba0b-11e9a989-00505692583a/FortiOS_6.2_AWS_Cookbook.pdf

QUESTION 4

Which two statements about Microsoft Azure network security groups are true? (Choose two.)

- A. Network security groups can be applied to subnets and virtual network interfaces.
- B. Network security groups can be applied to subnets only.
- C. Network security groups are stateless inbound and outbound rules used for traffic filtering.
- D. Network security groups are a stateful inbound and outbound rules used for traffic filtering.

Correct Answer: BD

Reference: <https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>

The screenshot shows the AWS Management Console interface for configuring Route Tables. The 'Route Tables' section is active, displaying a list of route tables. The 'Public-route' table is selected, and its configuration is shown below. The table has two routes: one for the destination 10.0.0.0/16 pointing to 'local', and another for 0.0.0.0/0 pointing to an Internet Gateway (igw-08e87b162f8182999).

Name	Route Table ID	Explicit subnet associator	Edge associations	Main	VPC ID	Owner
Private-route	rtb-040fce40e7029a32c	subnet-0c67f580822971d87	-	No	vpc-061d585389183ad02...	262226454685
Public-route	rtb-051b77e3c10a46085	subnet-08ffd4de2fbadfa72	-	Yes	vpc-061d585389183ad02...	262226454685

Destination	Target	Status
10.0.0.0/16	local	active
0.0.0.0/0	igw-08e87b162f8182999	active

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?

- A. 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.
- B. 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.
- C. 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.
- D. 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.

QUESTION 5

The screenshot displays two AWS EC2 instances in the Networking tab. The first instance, 'FortigateHA-FortiGate1', has a public IPv4 address field and a list of private IPv4 addresses: 10.0.4.11, 10.0.3.11, 10.0.1.11, and 10.0.0.11. The second instance, 'FortigateHA-FortiGate2', also has a public IPv4 address field and a list of private IPv4 addresses: 10.0.1.12, 10.0.0.12, 10.0.3.12, and 10.0.4.12.

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?



- 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.

Correct Answer: C

[NSE7_PBC-6.4 PDF Dumps](#)

[NSE7_PBC-6.4 Study
Guide](#)

[NSE7_PBC-6.4 Exam
Questions](#)