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.passapply.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

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

A. Proxy ARP entries are disregarded.

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

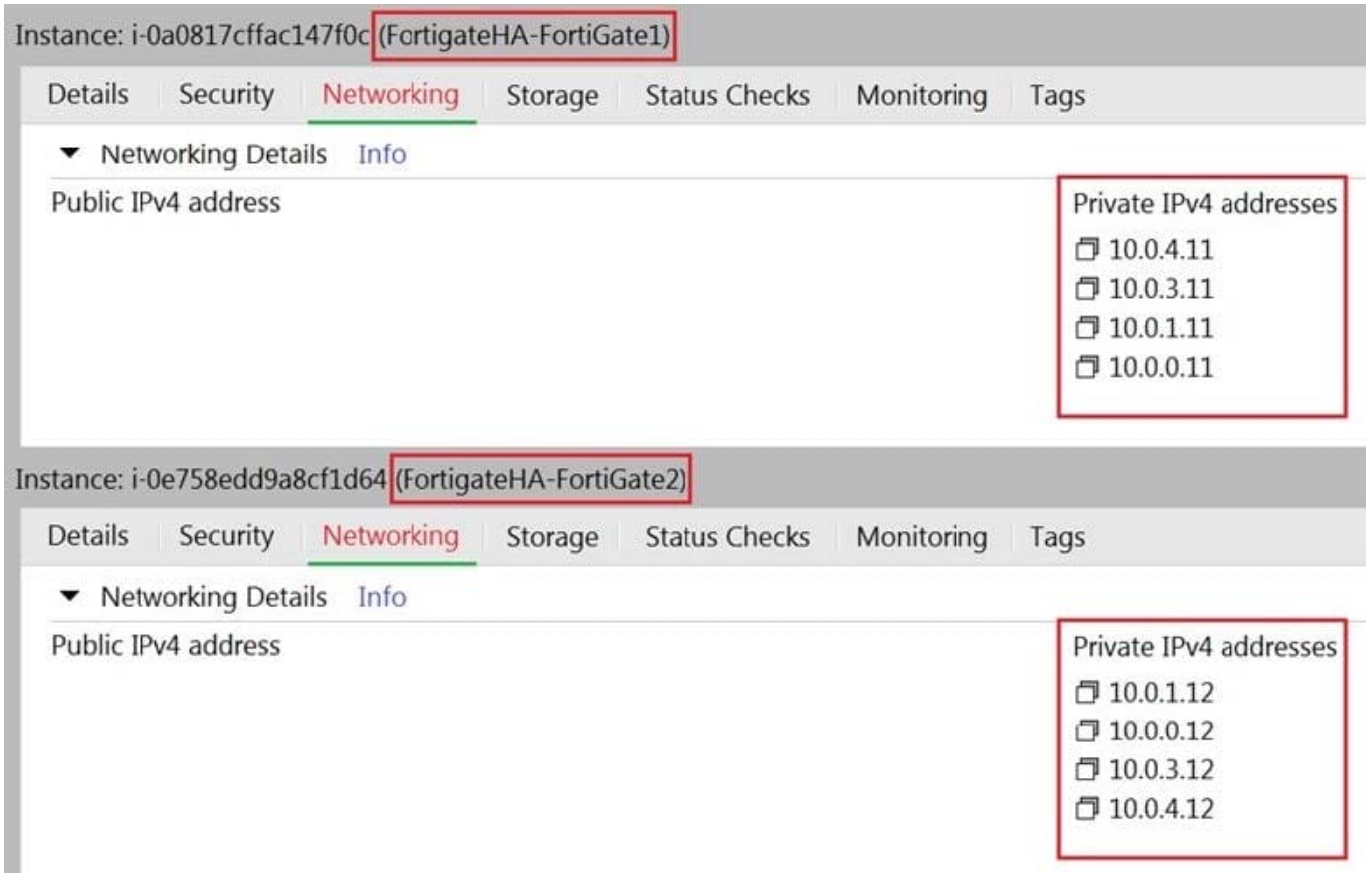
C. AWS DNS reserves the first host IP address of each subnet.

D. Multicast traffic is not allowed.

Correct Answer: CD

Reference: https://docs.aws.amazon.com/sdkfornet/v3/apidocs/items/EC2/TIEC2.html

QUESTION 2



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).

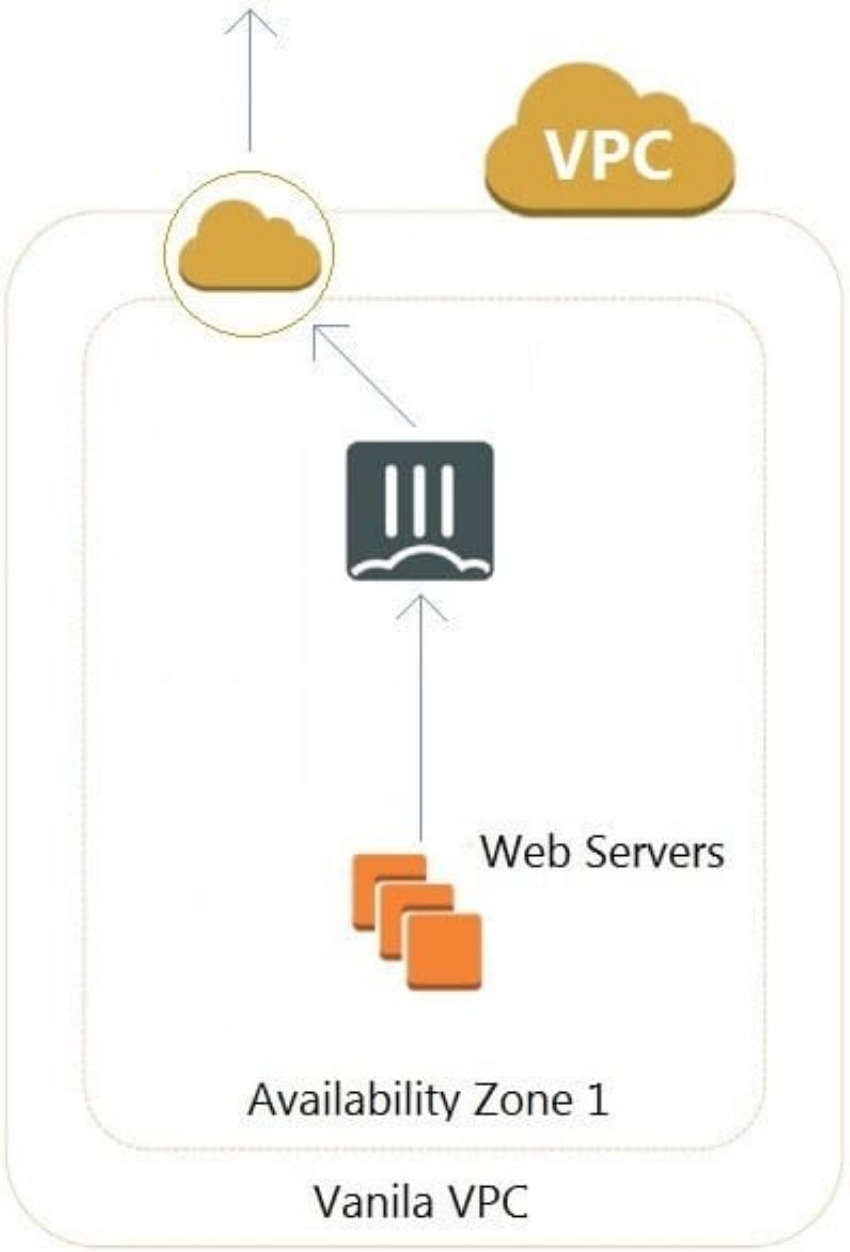
B. Delete the deployment and start again. You have in put the wrong parameters during the cloud formation template deployment.

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

QUESTION 3



Refer to the exhibit. A customer has deployed an environment in Amazon Web Services (AWS) and is now trying to send outbound traffic from the Web servers to the Internet. The FortiGate policies are configured to allow all outbound traffic; however, the traffic is not reaching the FortiGate internal interface.

What are two possible reasons for this behavior? (Choose two.)

A. The web servers are not configured with the default gateway.

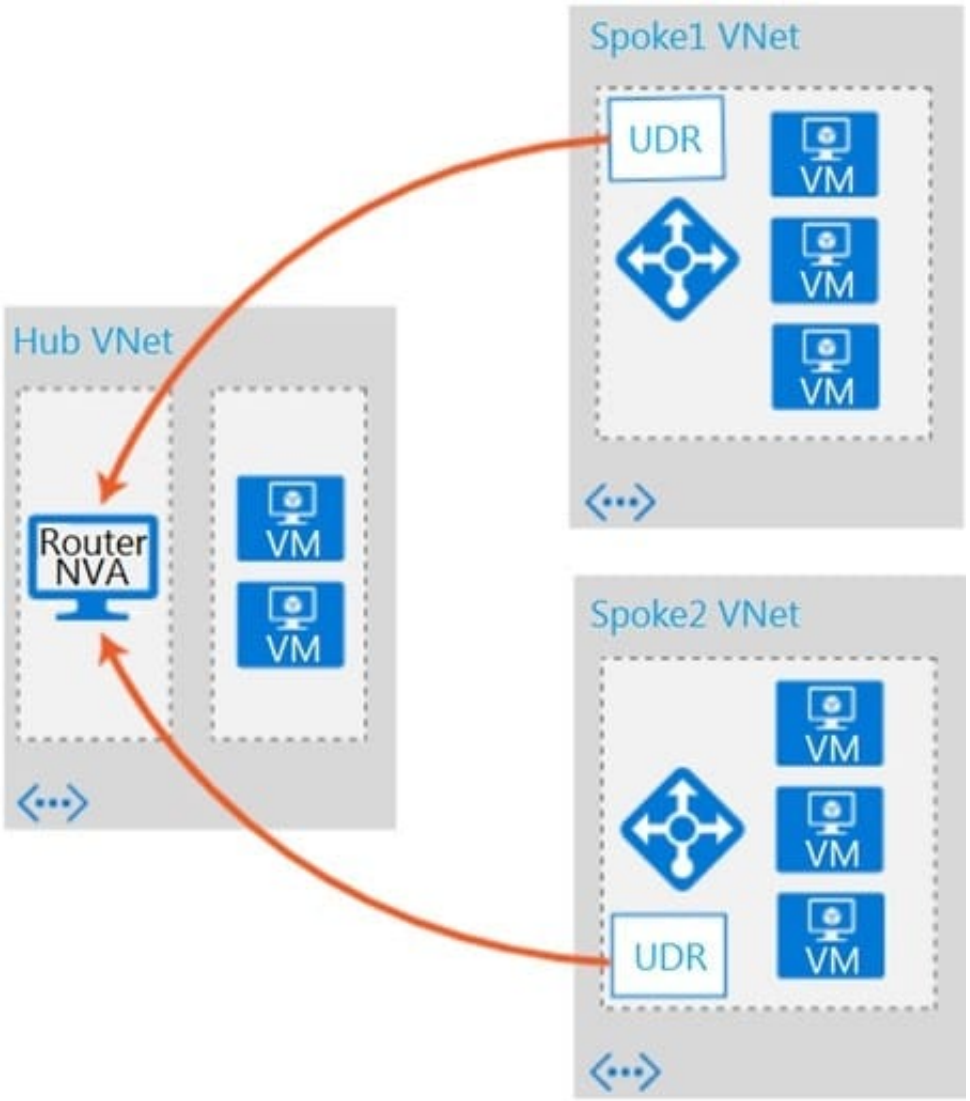
B. The Internet gateway (IGW) is not added to VPC (virtual private cloud).

C. AWS source and destination checks are enabled on the FortiGate interfaces.

D. AWS security groups may be blocking the traffic.

Correct Answer: AD

QUESTION 4



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.)

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.

Correct Answer: BD

QUESTION 5

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

What action will the worker node automatically perform to restore access to the black-holed subnet?

A. The worker node applies a route table from a non-black-holed subnet to the black-holed subnet.

B. The worker node moves the virtual IP of the terminated FortiGate to a running FortiGate on the worker node\\'s private subnet interface.

C. 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.

D. The worker node migrates the subnet to a different availability zone.

Correct Answer: D