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:

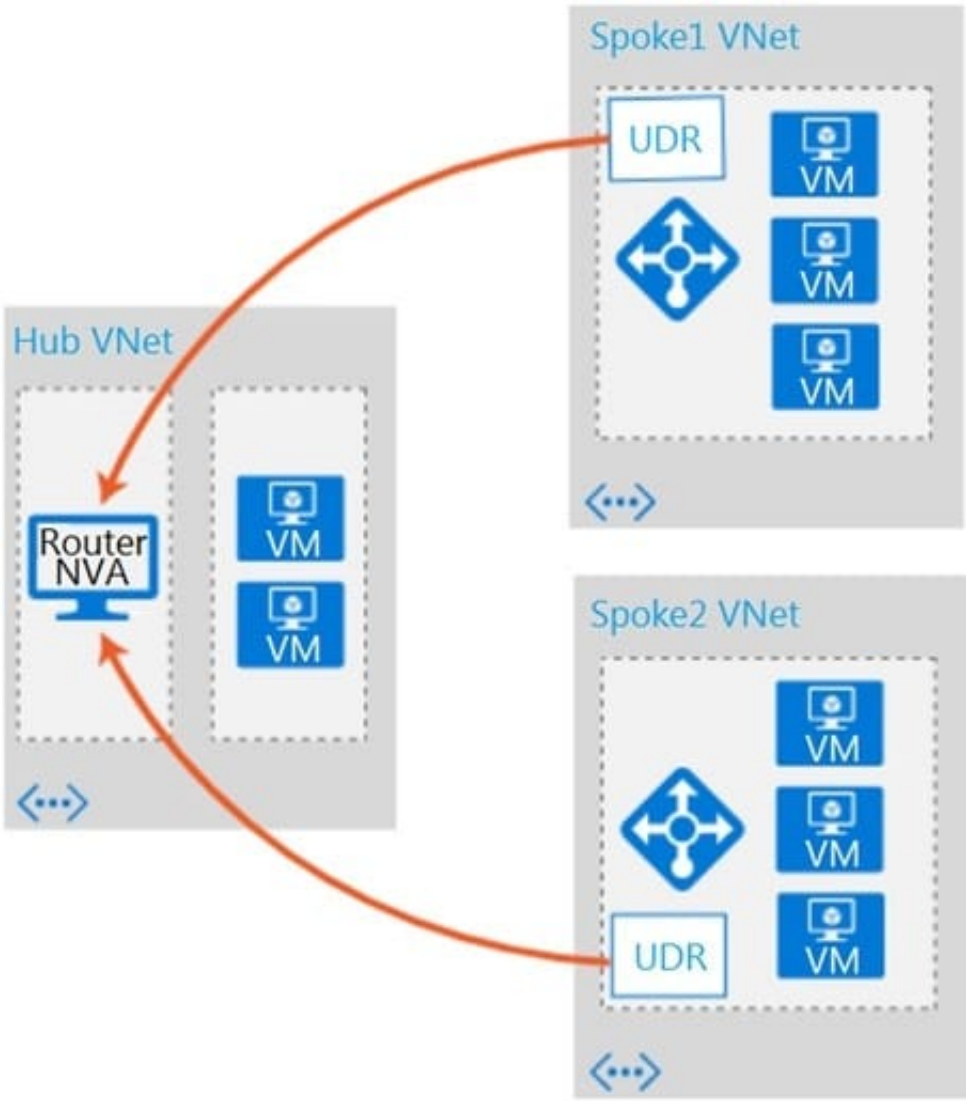
https://www.geekcert.com/nse7_pbc-6-4.html

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



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.

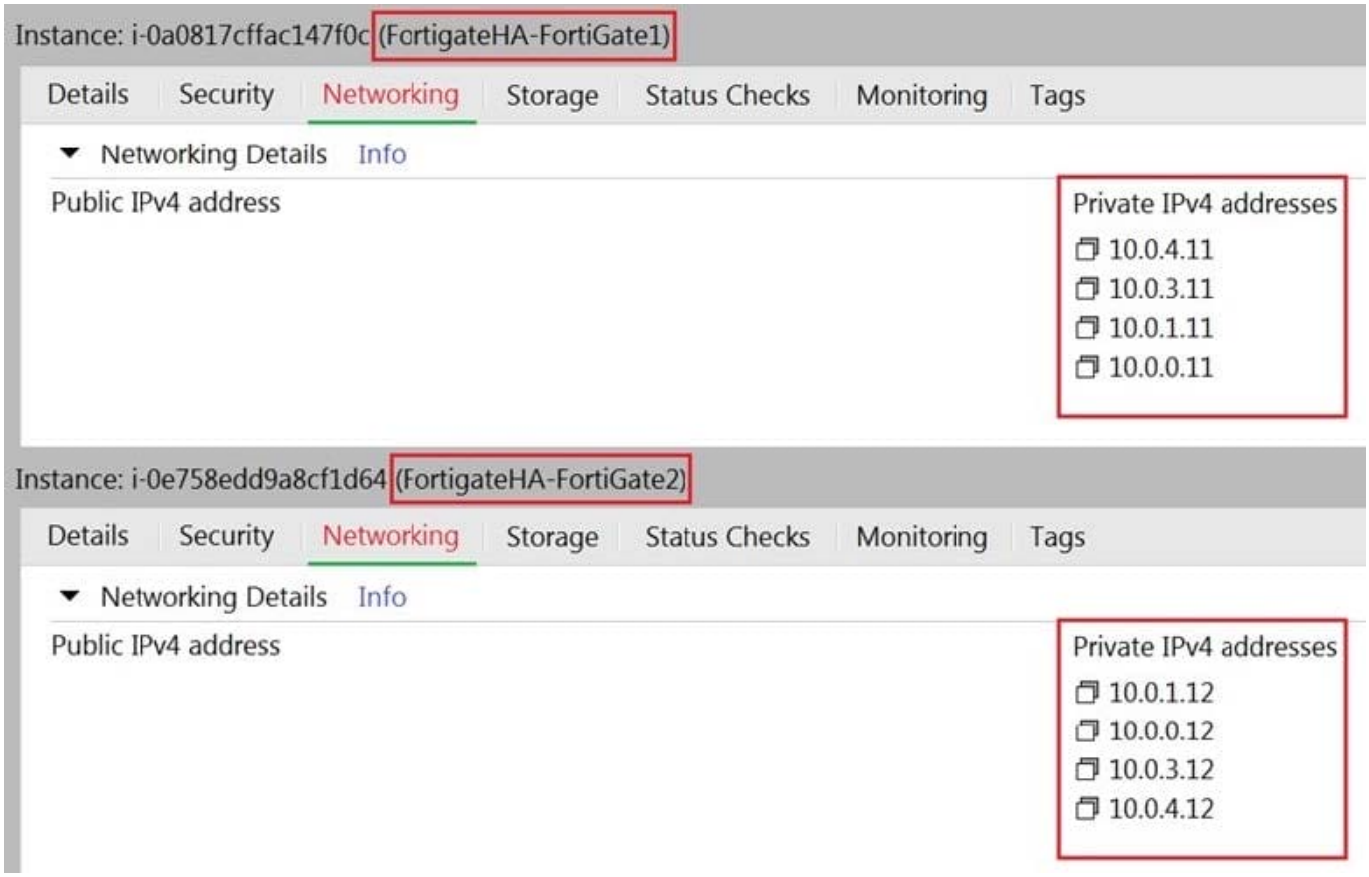
B. Use ExpressRoute to interconnect the hub VNets and spoke VNets.

C. Configure VNet peering between the spokes only.

D. Configure VNet peering between the hub and spokes.

Correct Answer: BD

QUESTION 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

When an organization deploys a FortiGate-VM in a high availability (HA) (active/active) architecture in Microsoft Azure, they need to determine the default timeout values of the load balancer probes.

In the event of failure, how long will Azure take to mark a FortiGate-VM as unhealthy, considering the default timeout values?

A. Less than 10 seconds

B. 30 seconds

C. 20 seconds

D. 16 seconds

Correct Answer: B

QUESTION 4

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 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