DUMPSARENA

Fortinet NSE 7 - Public Cloud Security 6.4

Fortinet NSE7_PBC-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

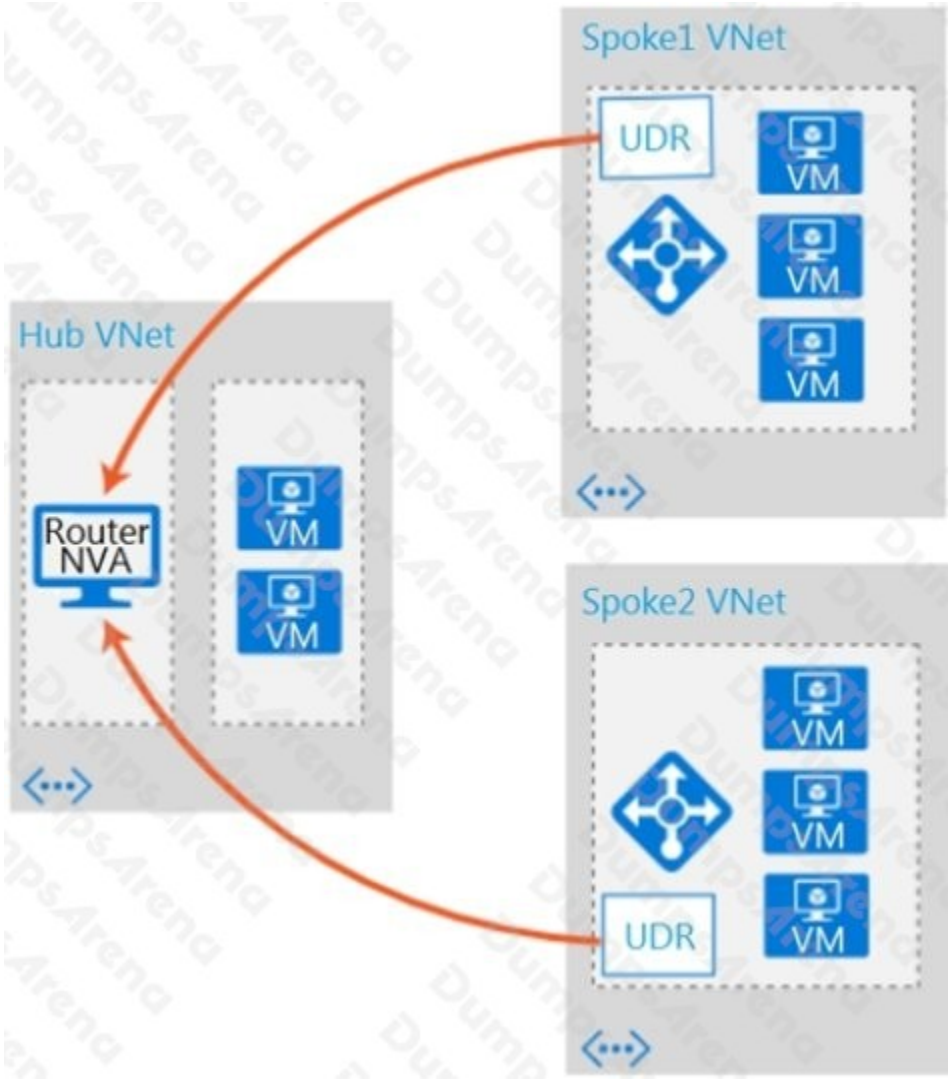
https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 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.

ANSWER: A D

QUESTION NO: 2

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.

ANSWER: B

Explanation:

GCP Limitations: You cannot add or remove network interfaces from an existing VM.
https://cloud.google.com/vpc/docs/create-use-multiple-interfaces#limitations

QUESTION NO: 3

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.

ANSWER: A D

Explanation:

https://blog.ipspace.net/2018/05/amazon-web-services-networking-overview.html

QUESTION NO: 4

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.

ANSWER: B

Explanation:

You must subscribe to GuardDuty, CloudWatch, S3, and DynamoDB. https://docs.fortinet.com/document/fortigate-public-cloud/6.4.0/aws-administration-guide/908646/populating-threat-feeds-with-guardduty

QUESTION NO: 5

You have previously deployed an Amazon Web Services (AWS) transit virtual private cloud (VPC) with a pair of FortiGate firewalls (VM04 / c4.xlarge) as your security perimeter. You are beginning to see high CPU usage on the FortiGate instances.

Which action will fix this issue?

A. Convert the c4.xlarge instances to m4.xlarge instances.

B. Migrate the transit VPNs to new and larger instances (VM08 / c4.2xlarge).

C. Convert from IPsec tunnels to generic routing encapsulation (GRE) tunnels, for the VPC peering connections.

D. Convert the transit VPC firewalls into an auto-scaling group and launch additional EC2 instances in that group.

ANSWER: D

Explanation:

Multiple FortiGate-VM instances form an Auto Scaling group to provide highly efficient clustering at times of high workloads. FortiGate-VM instances can be scaled out automatically according to predefined workload levels. https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/aws-administration-guide/397979/deploying-auto-scaling-on-aws