DUMPSQUEEN

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

dumpsqueen.com

QUESTION NO: 1

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: 2

When configuring the FortiCASB policy, which three configuration options are available? (Choose three.)

A. Intrusion prevention policies

B. Threat protection policies

C. Data loss prevention policies

D. Compliance policies

E. Antivirus policies

ANSWER: B C D

Explanation:

Policy setting allows you to configure each policy to fit the need of your usage. You can select any type of Policy (Data Analysis, Threat Protection or Compliance) https://docs.fortinet.com/document/forticasb/20.1.0/online-help/482958/policy-configuration

QUESTION NO: 3

Which two Amazon Web Services (AWS) topologies support east-west traffic inspection within the AWS cloud

by the FortiGate VM? (Choose two.)

A. A single VPC deployment with multiple subnets and a NAT gateway

B. A single VPC deployment with multiple subnets

C. A multiple VPC deployment utilizing a transit VPC topology

D. A multiple VPC deployment utilizing a transit gateway

ANSWER: C D

Explanation:

Multi-VPC design. AWS recommends segmenting networks at the VPC level. In this approach, workloads are grouped together at the VPC level instead of the subnet level. All traffic between VPCs will be inspected by network security virtual firewalls at each VPC or at a shared VPC. Design patterns such as Transit VPC or AWS Transit Gateway can be used to achieve this in an automated and scalable fashion.

QUESTION NO: 4

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: 5

Which statement about FortiSandbox in Amazon Web Services (AWS) is true?

A. In AWS, virtual machines (VMs) that inspect files do not have to be reset after inspecting a file.

B. FortiSandbox in AWS uses Windows virtual machines (VMs) to inspect files.

C. In AWS, virtual machines (VMs) that inspect files are constantly up and running.

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

ANSWER: B

Explanation:

FortiSandbox deploys new EC2 instances with the custom Windows VMs, and then it sends malware, runs it, and captures the results for analysis. FortiSandbox for AWS does not need more resources because it performs management and analysis tasks only. Note that the cost varies based on the number of EC2 instances deployed, size of the instances, and duration of the running time.