Fortinet

NSE7_PBC-6.4
Fortinet NSE 7 - Public Cloud Security 6.4

For More Information – Visit link below:
https://www.examsempire.com/

Product Version

1. **Up to Date products, reliable and verified.**
2. **Questions and Answers in PDF Format.**

https://examsempire.com/

Latest Version: 8.0

Question: 1

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: BCD

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: 2

You have been tasked with deploying FortiGate VMs in a highly available topology on the Amazon Web Services (AWS) cloud. The requirements for your deployment are as follows:
• You must deploy two FortiGate VMs in a single virtual private cloud (VPC), with an external elastic load balancer which will distribute ingress traffic from the internet to both FortiGate VMs in an active-active topology.
• Each FortiGate VM must have two elastic network interfaces: one will connect to a public subnet and other will connect to a private subnet.
• To maintain high availability, you must deploy the FortiGate VMs in two different availability zones.
How many public and private subnets will you need to configure within the VPC?

A. One public subnet and two private subnets
B. Two public subnets and one private subnet
C. Two public subnets and two private subnets
D. One public subnet and one private subnet

Answer: C

Explanation:
https://github.com/fortinet/aws-cloudformation-templates/blob/master/LambdaAARouteFailover/6.0/README.md
https://github.com/fortinet/aws-cloudformation-templates/tree/master/LambdaAA-RouteFailover/6.0

Question: 3

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?

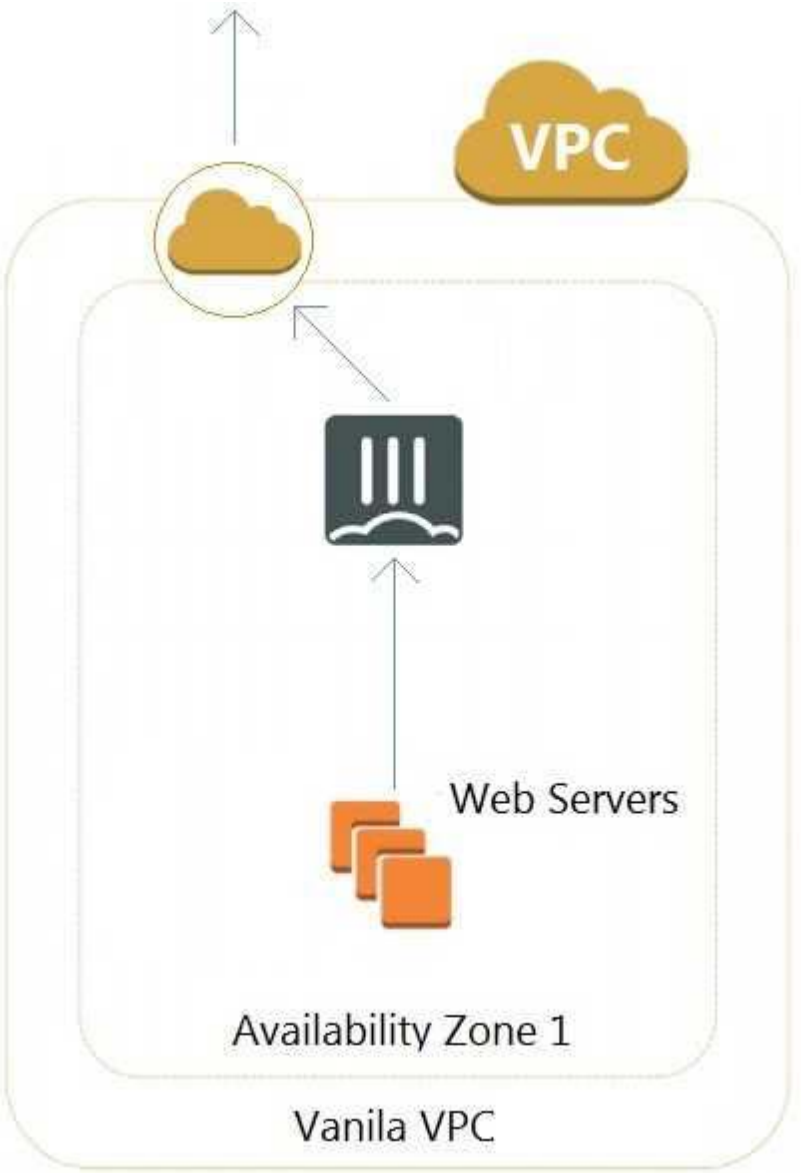
A. GuardDuty, CloudWatch, S3, Inspector, WAF, and Shield.
B. GuardDuty, CloudWatch, S3, and DynamoDB.
C. Inspector, Shield, GuardDuty, S3, and DynamoDB.
D. WAF, Shield, GuardDuty, S3, and DynamoDB.

Answer: B

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

Question: 4

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.)

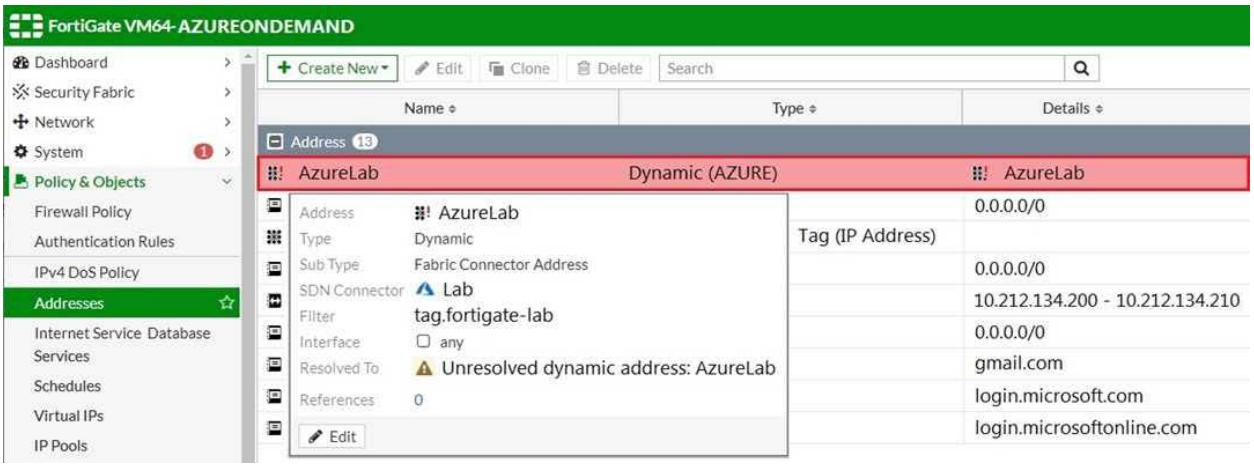
A. The web servers are not configured with the default gateway.
B. The Internet gateway (IGW) is not added to VPC (virtual private cloud).
C. AWS source and destination checks are enabled on the FortiGate interfaces.
D. AWS security groups may be blocking the traffic.

Answer: CD

Explanation:
You need to check if source/destination are enabled. Public_Cloud_6.4_Study_Guide Page 67

Question: 5

Refer to the exhibit.



Your senior administrator successfully configured a FortiGate fabric connector with the Azure resource manager, and created a dynamic address object on the FortiGate VM to connect with a windows server in Microsoft Azure. However, there is now an error on the dynamic address object, and you must resolve the issue.
How do you resolve this issue?

A. Run diagnose debug application azd -l on FortiGate.
B. In the Microsoft Azure portal, set the correct tag values for the windows server.
C. In the Microsoft Azure portal, access the windows server, obtain the private IP address, and assign the IP address under the FortiGate-VM AzureLab address object.
D. Delete the address object and recreate a new address object with the type set to FQDN.

Answer: B

Explanation:
https://docs.fortinet.com/document/fortigate-public-cloud/6.2.0/azure-administrationguide/985498/troubleshooting-azure-fabric-connector

Thank You for Trying Our Product

Discount Coupon Code is: 20OFF2022

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/