NEO DUMPS

Fortinet

NSE7_PBC-6.4 Exam

NSE 7

Questions & Answers

(Demo Version - Limited Content)

Thank you for Downloading NSE7_PBC-6.4 exam PDF Demo

Get Full File:

https://neodumps.com/nse7_pbc-6-4/

WWW.NEODUMSP.COM

Version: 4.0

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

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/bf017449-572a-11e9- 81a4-00505692583a/forticasb-4.1.0-admin-guide.pdf (62)

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: A

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.

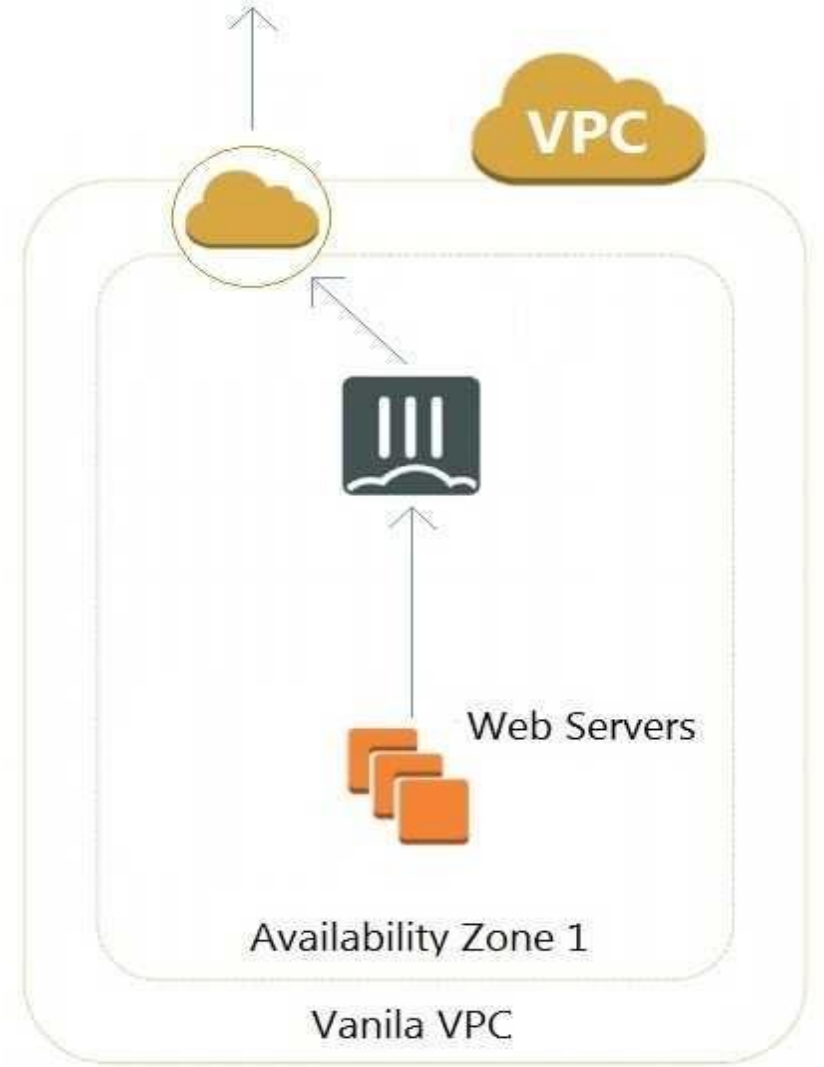
D. WAF, Shield, GuardDuty, S3, and DynamoDB.

Answer: A

Reference: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/ed901ad2-4424-11e9- 94bf-00505692583a/FortiOS_6.2.0_AWS_Cookbook.pdf

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.

www.neodumps.com

Thank You for trying NSE7_PBC-6.4 PDF Demo

https://neodumps.com/nse7_pbc-6-4/

Start Your NSE7_PBC-6.4 Preparation

[Limited Time Offer] Use Coupon "SAVE20" for extra 20% discount on the purchase of PDF file. Test your NSE7_PBC-6.4 preparation with actual exam questions