

DUMPSBOSS.

**Fortinet NSE 6 Securing AWS with Fortinet
Cloud Security 6.4**

Fortinet NSE6 WCS-6.4

Version Demo

Total Demo Questions: 5

Total Premium Questions: 30

Buy Premium PDF

<https://dumpsboss.co>

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Refer to the exhibit.

```
Fgt2 # diagnose debug enable

Fgt2 # diagnose debug application awsd -1
Debug messages will be on for 30 minutes.

Fgt2 # HA event
HA state: master
send_vip_arp: vd root master 1 intf port1 ip 10.0.0.13
send_vip_arp: vd root master 1 intf port2 ip 10.0.1.13
send_vip_arp: vd root master 1 intf fortilink ip 169.254.1.1
awsd get instance id i-0428502a5884d0987
awsd get iam role FortiGateHA-InstanceRole-1U05GGE537X83
awsd get region us-east-2
awsd get vpc id vpc-0e3cf73524e2f8b4e
```

You deployed an active-passive FortiGate HA using a Cloud Formation template on an existing VPC_ Now you want to test active-passive FortiGate HA failover by

running a debug so you can see the API calls to change the elastic and secondary IP addresses.

Which statement is correct about the output of the debug?

- A. The routing table for Fgt2 updated successfully. and port2 will provide internet access to Fgt2.
- B. The elastic IP is associated with port1 of Fgt2.
- C. IP address 10. 0. 0. 1 3 is now associated with eni-Ob61d8afcOaefb8a2.
- D. The elastic IP is associated with port2 of Fgt2. and the secondary IP address for port1 and port2 was updated successfully.

ANSWER: C

QUESTION NO: 2

A customer deployed Fortinet Managed Rules for Amazon Web Services (AWS) Web-Application Firewall (WAF) to protect web application servers from attacks.

Which statement about Fortinet Managed Rules for AWS WAF is correct?

- A. It offers a negative security model.
- B. It can provide Layer 7 DOS protection.
- C. It can provide IP Reputation (WAF subscription FortiGuard).

D. It can perform bot and known search engine identification and protection

ANSWER: D

QUESTION NO: 3

Which three statements are correct about VPC flow (Choose three.)

- A. Flow logs can capture real-time log streams for the network interfaces.
- B. Flow logs do not capture DHCP traffic.
- C. Flow logs can capture traffic to the reserved IP address for the default VPC router.
- D. Flow logs can be used as a security tool to monitor the traffic that is reaching the instance.
- E. Flow logs do not capture traffic to and from 169.254.169.254 for instance metadata.

ANSWER: B D E

QUESTION NO: 4

Which three statements are correct about AWS security groups? (Choose three)

- A. a Security group rules are always permissive: you cannot create rules that deny access.
- B. By default, security groups block all outbound traffic.
- C. When associate multiple security groups With an instance, the rules from each security group are effectively aggregated to create one set Of rules
- D. Security groups are statetul
- E. By default, security groups allow all inbound traffic.

ANSWER: A C D

QUESTION NO: 5

You connected to the AWS Management Console at 10:00 AM and verified that there are two FortiGate VMS running, You receive a call from a user reporting about a temporary slow Internet connection that lasted only a few minutes. When you go

back to the AWS portal. you notice there are now two additional FortiGate VMS that you did not create. Later that day, the number of VMS returns to two without your intervention. A similar situation occurs several times during the week.

What is the most likely reason for this to happen?

- A. The VMS are in an availability group with dynamic membership.
- B. Autoscaling is configured to act as described in the scenario.
- C. The user ran a script to create the extra VMS to get faster connectivity.
- D. The AWS portal is not refreshed automatically. and another administrator is creating and removing the VMS as needed.

ANSWER: B