Question 1

An administrator has deployed an environment in AWS and is now trying to send outbound traffic from the web servers to the internet through FortiGate. The FortiGate policies are configured to allow all outbound traffic. however. the traffic is not reaching the FortiGate internal interface.

Which two statements Can be the reasons for this behavior? (Choose two)

A. FortiGate is not configured as a default gateway tor web servers.

B. Internet Gateway (IGW) is not configured for VPC.

C. AWS security groups are blocking the traffic.

D. AWS source destination checks are enabled on the FortiGate internal interfaces.

Answer: CD

Explanation:

Question 2

You are network connectivity issues between two VMS deployed in AWS. One VM is a FortiGate located on subnet •LAN- that is part Of the VPC "Encryption". The Other VM is a Windows server located on the subnet "servers" Which is also in the "Encryption" VPC. You are unable to ping the Windows server from FortiGate.

What is the reason for this?

A. You have not created a VPN to allow traffic between those subnets.

B. By default. AWS does not allow ICMP traffic between subnets.

C. The default AWS Network Access Control List (NACL) does not allow this traffic.

D. The firewall in the Windows VM is blocking the traffic.

Answer: D

Explanation:

Question 3

Your company deployed a FortiSandb0X for AWS.

Which statement is correct about FortiSandbox for AWS?

A. FortiSandbox for AWS does not need more resources because it performs only management and analysis tasks.

B. The FortiSandbox manager is installed on AWS platform and analyzes the results of the sandboxing process received from on-premises Windows instances.

C. FortiSandbox for AWS comes as hybrid solution. The FortiSandb0X manager is installed onpremises and analyzes the results Of the sandboxing process received from AWS EC2 instances

D. FortiSandbox deploys new EC2 instances with the custom Windows and Linux VMS, then it sends malware, runs it, and captures the results for analysis.

Answer: A

Explanation:

Question 4

An organization has created a VPC and deployed a FortiGate-VM (VM04 /c4.xlarge) in AWS, FortiGate-VM is initially configured With two Elastic Network Interfaces

(ENIs). The primary ENI of FortiGate-VM is configured for a public subnet. and the second ENI is configured for a private subnet. In order to provide internet access. they now want to add an EIP to the primary ENI of FortiGate, but the EIP assignment is failing.

Which action would allow the EIP assignment to be successful?

A. Shut down the FortiGate VM. if it is running. assign the EIP to the primary ENI. and then power it on.

B. Create and associate a public subnet With the primary ENI Of FortiGate, and then assign the EIP to the primary ENI.

C. Create and attach a public routing table to the public subnet, associate the public subnet With the primary ENI Of FortiGate. and then assign the EP to the primary ENI.

D. Create and attach an Internet gateway to the VPC. and then assign the EIP to the primary ENI Of FortiGate.

Answer: D

Explanation:

Question 5

HOW is traffic failover handled in a FortiGate active-active cluster deployed in AWS?

A. The elastic load balancer handles traffic failover using FGCP.

B. The elastic load balancer handles bi-directional traffic failover using a health probe.

C. All FortiGate cluster members send health probes using a dedicated interface.

D. All FortiGate cluster members use unicast FGCP_

Answer: B

Explanation:

Question 6

Which AWS product integrates With FortiGate to automate security remediation for workloads running on the AWS platform?

A. AWS Protector

B. AWS Inspector

C. AWS Shield

D. AWS GuardDuty

Answer: D

Explanation:

Question 7

A customer deployed an HA Cloud formation to Stage and bootstrap the FortiGate configuration.

Which AWS functions are used by FortiGate HA to call the HA failover?

A. AWS Lambda functions

B. AWS Mapping functions

C. AWS S3 functions

D. AWS DynamoDB functions

Answer: A

Explanation:

Question 8

What is the purpose of the created as part Of a FortiGate autoscale deployment using Fortinet cloud formation template in AWS?

A. To store information about varying states of auto scaling conditions.

B. To Store the information used for the scale set.

C. To store the traffic logs Of all FortiGates.

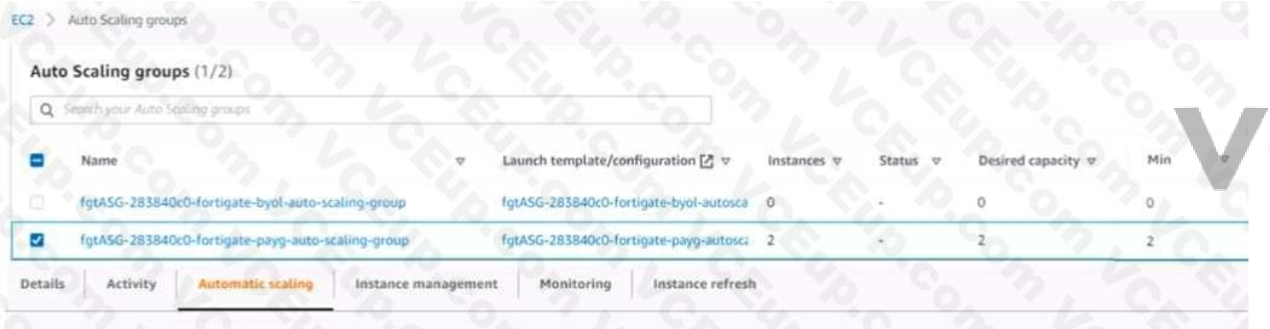
D. To store the firewall policies used by all FortiGates_

Answer: A

Explanation:

Question 9

Refer to the exhibit.



EC2 > Auto Scaling groups
Auto Scaling groups (1/2)
Search your Auto Scaling groups
Details
Activity
Automatic scaling
Instance management
Monitoring
Instance refresh

	Name	Launch template/configuration	Instances	Status	Desired capacity	Min
□	fgtASG-283840c0-fortigate-byol-auto-scaling-group	fgtASG-283840c0-fortigate-byol-autosca	0	-	0	0
☑	fgtASG-283840c0-fortigate-payg-auto-scaling-group	fgtASG-283840c0-fortigate-payg-autosc:	2	-	2	2

An administrator configured two auto-scaling polices that they now want to test, What Will be the impact on payg-auto-scaling-group for the FortiGate devices if the administrator executes a scale-in policy?

A. The scale-in policy will decrease instances from two to one.

B. The scale-in policy will decrease the desired capacity from two to one

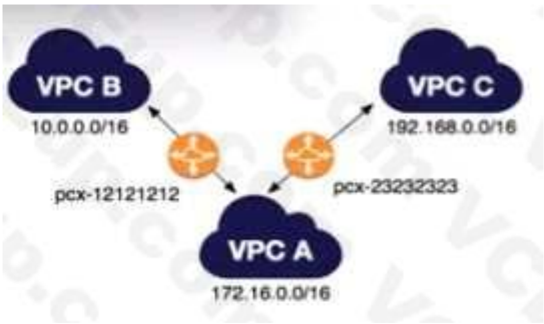
C. The scale-in policy will decrease the number of maximum instances from four to three.

Answer: C

Explanation:

Question 10

Refer to the exhibit.



Which statement is correct about the VPC peering connections shown in the exhibit?

A. You can associate VPC ID pcx-23232323 with VPC B to form a VPC peering connection between VPC B and VPC C.

B. You cannot route packets directly from VPC B to VPC C through VPC A.

C. TO route packets directly from VPC B to VPC C through VPC A, you must add a route for network 192.168.0.0/16 in the VPC A routing table.

D. You cannot create a VPC peering connection between VPC B and VPC C to route packets directly.

Answer: B

Explanation:

Question 11

A customer needs a recursive DNS for AWS VPC and on-premises networks, The customer also wants to create conditional forwarding rules and DNS endpoints to resolve custom names in AWS private hosted zones and on-premises DNS servers.

Which Amazon service can be used to achieve this scenario?

A. AWS mapping service

B. Amazon route 53

C. AWS DynamoOB service

D. AWS Lambda service

Answer: B

Explanation:

Question 12

Which product you Can use as AWS WAF web access control lists (web ACLS) to minimize the effects Of a DDOS attack?

A. AWS Protector

B. AWS GuardDuty

C. AWS Inspector

D. AWS Shield

Answer: D

Explanation:

Question 13

As part of the security plan you have been tasked with deploying a FortiGate in AWS.

Which two are the security responsibility of the customer in a cloud environment? (Choose two.)

A. Virtualization platform

B. Traffic encryption

C. User management

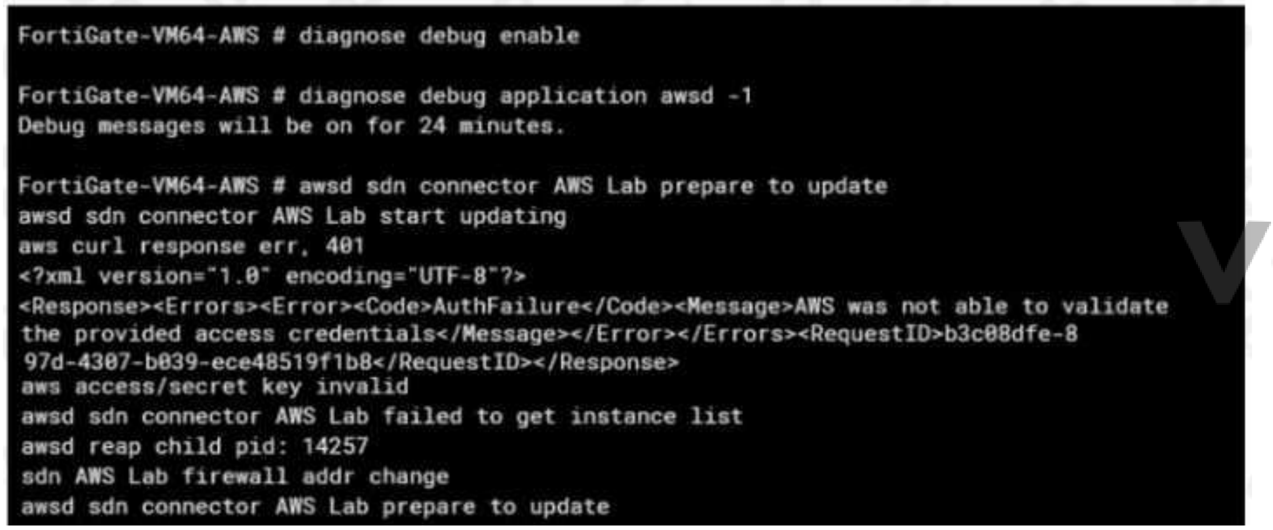
D. Storage infrastructure

Answer: BC

Explanation:

Question 14

Refer to the exhibit.



```
FortiGate-VM64-AWS # diagnose debug enable

FortiGate-VM64-AWS # diagnose debug application awsd -1
Debug messages will be on for 24 minutes.

FortiGate-VM64-AWS # awsd sdn connector AWS Lab prepare to update
awsd sdn connector AWS Lab start updating
aws curl response err, 401
<?xml version="1.0" encoding="UTF-8"?>
<Response><Errors><Error><Code>AuthFailure</Code><Message>AWS was not able to validate
the provided access credentials</Message></Error></Errors><RequestID>b3c08dfe-8
97d-4307-b039-ece48519f1b8</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14257
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab prepare to update
```

An administrator configured a FortiGate device to connect to me AWS API to retrieve resource values from the AWS console to create dynamic objects tor the FortiGate policies. The administrator is unable to retrieve AWS dynamic objects on FortiGate.

Which three reasons can explain btw? (Choose three.)

A. AWS was not able to validate credentials provided by the AWS Lab SON connector.

B. The AWS Lab SON connector failed to connect on port 401.

C. The AWS Lab SON connector failed to retrieve the instance list.

D. The AWS API call is not supported on XML version I . O.

E. The AWS Lab SON connector is configured with an invalid AWS access or secret key

Answer: ACE

Explanation:

Question 15

Which statement is true about an Elastic Network Interface (ENI)?

A. Once ENI detaches from one instance. it cannot reattach to another instance.

B. You can detach primary ENI from an AWS instance.

C. An ENI cannot move between AZs.

D. When you move an ENI, network traffic is not redirected to the new instance.

Answer: C

Explanation:

Question 16

Which two statements are correct about AWS Network Access Control Lists (NACLS)? (Choose two.)

A. NACLs are stateless: responses to allowed inbound traffic are subject to the rules for outbound traffic.

B. An NACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.

C. By default. each custom NACL allows all inbound and outbound traffic unless you add new rules,

D. VPC automatically comes with a modifiable default NACL, and by default it denies all inbound and outbound IPv4 traffic.

Answer: AB

Explanation:

Question 17

Which features are only available on FortiWeb when compared to Fortinet Managed Rules for AWS WAF?

A. FortiWeb meets PCI 6.6 compliance.

B. FortiWeb can scan web application vulnerabilities.

C. FortiWeb provides a WAF subscription (FortiGuard) option.

D. FortiWeb provides web application attack signatures.

Answer: B

Explanation:

Question 18

Which three Fortinet products are available in Amazon Web Services in both on-demand and bring your own license (BYOL) formats? (Choose three.)

A. FortiGate

B. FortiWeb

C. FortiADC

D. FortiSIEM

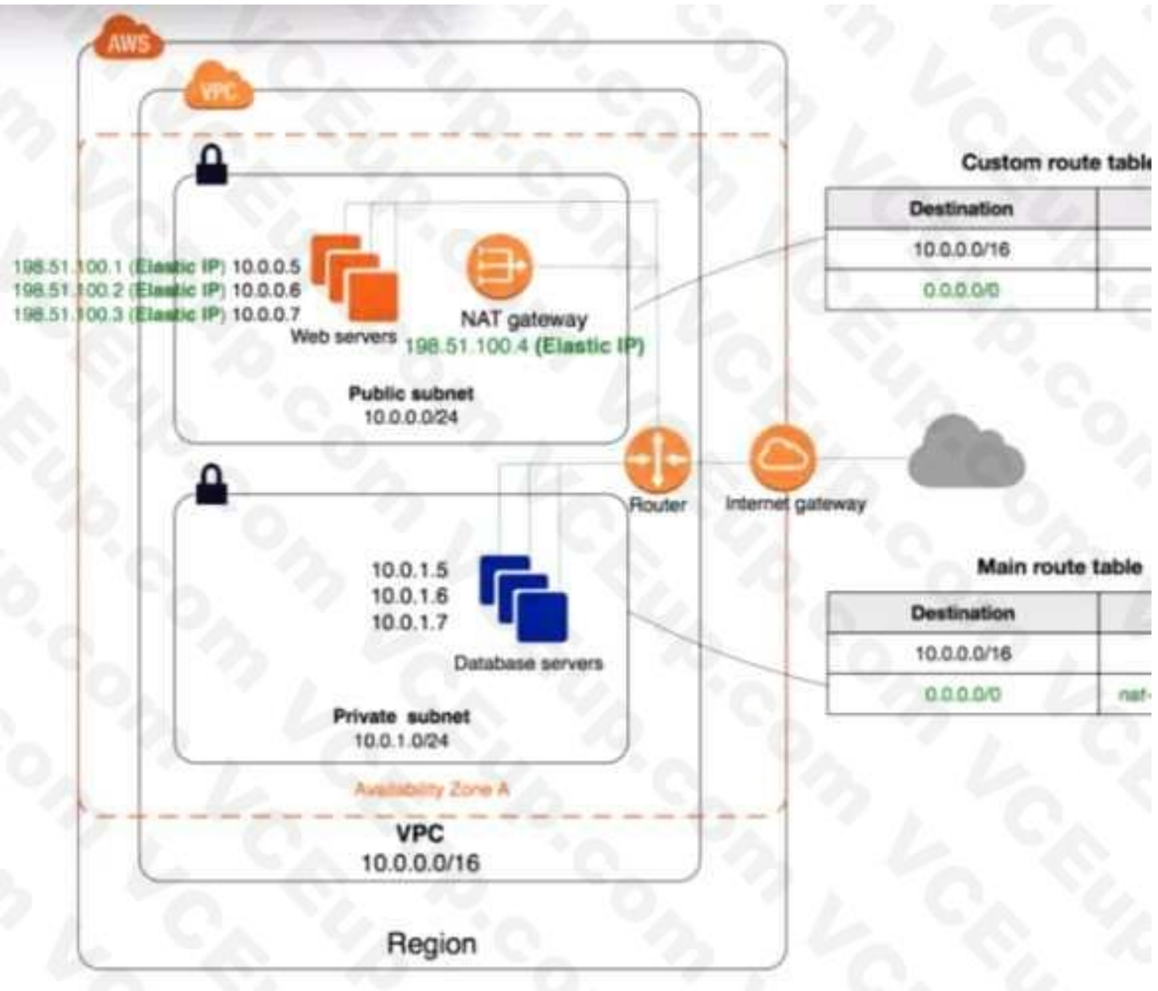
E. FortiSOAR

Answer: ABC

Explanation:

Question 19

Refer to the exhibit.



Custom route tabl

Destination	
10.0.0.0/16	
0.0.0.0/0	

Main route table

Destination	
10.0.0.0/16	
0.0.0.0/0	nat-

An administrator wants to update the database package from the Internet to a database server configured with IP address Which statement is correct about traffic from server IP address 10.0.1.7 to the internet. based on the diagrarm?

A. Traffic from server 10.0.1.7 to the internet will hide behind elastic IP 198.51.100 2.

B. Traffic from server 10.0.1.7 to the internet will hide behind elastic IP 198.51.100.3

C. Traffic from server 10.0.1.7 to the internet will hide behind elastic IP 198.51.100.4

D. Traffic from server 10.0.1.7 to the internet will hide behind elastic IP 198.51.100.1

Answer: C

Explanation:

Question 20

An MSSP deployed 16 FortiGate VMS With the default AWS security groups and network access lists using an on-demand license from Amazon Web Services (AWS) Marketplace. They are using a thirdparty configuration backup application to back up and track changes for the FortiGate configurations.

It can connect to the FortiGate devices using only the SSH protocol, A customer is using the correct username and password configured on the FortiGate devices. but they are unable to log in using the SSH protocol.

What can be the reason Why this authentication is failing?

A. The default AWS network access list for FortiGate does not allow SSH.

B. The AWS key is required to log in to FortiGate using SSH

C. AWS uses non-standard SSH port 1025, and the default AWS security groups and NACL for FortiGate are not configured for the port.

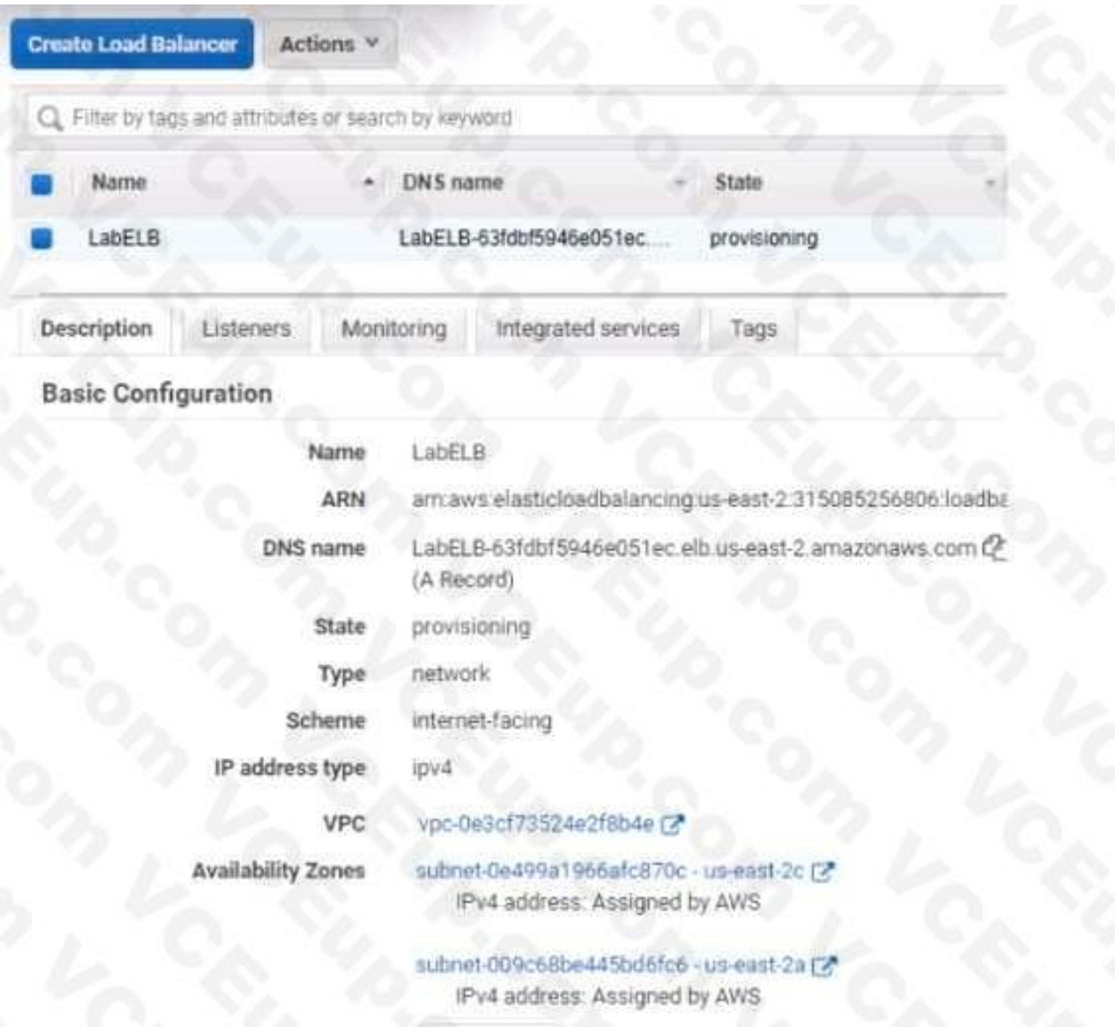
D. The default AWS Security group for FortiGate does not allow SSH.

Answer: B

Explanation:

Question 21

Refer to the exhibit.



Name	DNS name	State
LabELB	LabELB-63fdbf5946e051ec....	provisioning

Basic Configuration

Name	LabELB
ARN	arn:aws:elasticloadbalancing:us-east-2:315085256806:loadba
DNS name	LabELB-63fdbf5946e051ec.elb.us-east-2.amazonaws.com (A Record)
State	provisioning
Type	network
Scheme	internet-facing
IP address type	ipv4
VPC	vpc-0e3cf73524e2f8b4e
Availability Zones	subnet-0e499a1966afc870c - us-east-2c IPv4 address: Assigned by AWS subnet-009c68be445bd6fc6 - us-east-2a IPv4 address: Assigned by AWS

A customer is using the AWS Elastic Load Balancer.

Which two statements are correct about the Elastic Load Balancer configuration? (Choose two.)

A. The Amazon resource name is used to access the load balancer node and targets.

B. The DNS name is used to access devices.

C. The load balancer is configured to load balance traffic between devices in two AZS.

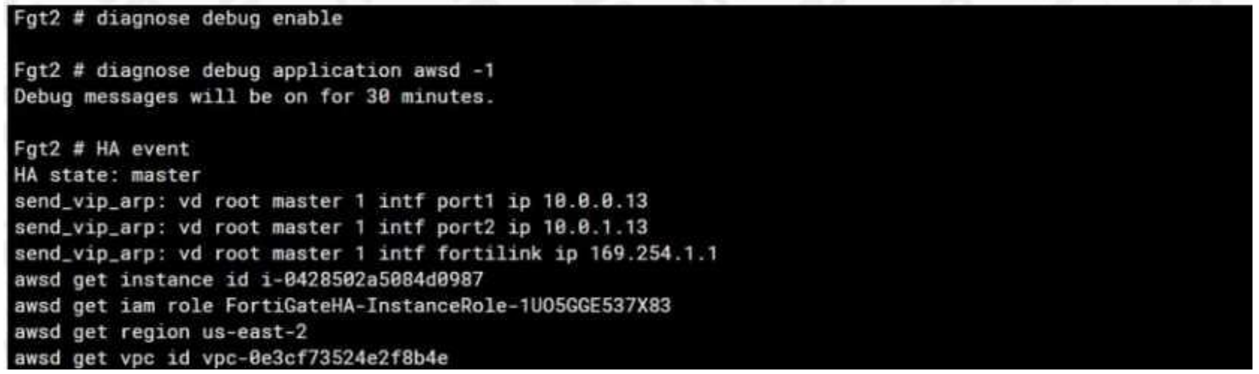
D. The load balancer is configured for the internal traffic of the VPC

Answer: BC

Explanation:

Question 22

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-0428502a5084d0987
awsd get iam role FortiGateHA-InstanceRole-1UO5GGE537X83
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. O. O. L 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

Explanation:

Question 23

You want to deploy FortiGate for AWS to protect your production network in the cloud. but you do not need the 2417 support available in the enterprise bundle.

Which license model do you choose?

A. pay as you go (PAYG).

B. Bring your own device (BYOD)

C. Bring your own license (BYOL).

D. Pay as a bundle (PAYB).

Answer: A

Explanation:

Question 24

You want to deploy the Fortinet HA cloud formation template to stage and bootstrap the FortiGate configuration in the same that you created your VPC, Which is Ohio US-East-2.

Based on this information, Which statement is correct?

A. You must create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration in the Ohio US-East-2 region.

B. You must create an S3 bucket to stage and bootstrap FortiGate with an FGCP multicast configuration in the Ohio US-East-2 region.

C. You must create an S3 bucket to stage and bootstrap FortiGate with an FGCP unicast configuration in any region.

D. The Fortinet HA cloud formation template automatically creates an S3 bucket.

Answer: D

Explanation:

Question 25

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

Explanation:

Question 26

Which three statements are correct about Amazon Web Services networking? (Choose three.)

A. You can configure instant IP failover in AWS.

B. You cannot configure gratuitous ARP but you can configure proxy ARP.

C. You cannot deploy FortiGate in transparent mode in AWS.

D. You cannot use custom frames in AWS

E. You can use unicast the FGCP protocol

Answer: CDE

Explanation:

Question 27

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.

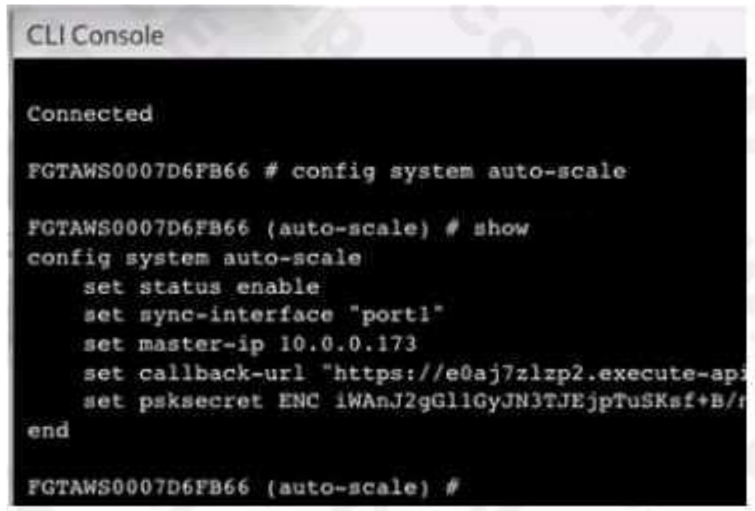
E. Flow logs do not capture traffic to and from 169.2 54 .169.254 for instance metadata.

Answer: BDE

Explanation:

Question 28

Refer to the exhibit.



```
Connected

FGTAWS0007D6FB66 # config system auto-scale

FGTAWS0007D6FB66 (auto-scale) # show
config system auto-scale
    set status enable
    set sync-interface "port1"
    set master-ip 10.0.0.173
    set callback-url "https://e0aj7zlzp2.execute-api
    set psksecret ENC iWAnJ2gGl1GyJN3TJEjpTuSKsf+B/r
end

FGTAWS0007D6FB66 (auto-scale) #
```

You have created an autoscale configuration using a FortiGate HA Cloud Formation template. You want to examine the autoscale FortiOS configuration to confirm that FortiGate autoscale is configured to synchronize primary and secondary devices. On one of the FortiGate devices, you execute the command shown in the exhibit Which statement is correct about the output of the command?

A. The device is the primary in the HA configuration. with the IP address 10.0.0.173.

B. The device is the secondary in the HA configuration, and the IP address Of the primary device is 10.0.0.173.

C. The device is the primary in the HA configuration and the IP address of the secondary device is 10.0.0.173.

D. The device is the secondary in the HA configuration. with the IP address 10.0.0.173.

Answer: B

Explanation:

Question 29

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

Explanation:

Question 30

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: ACD

Explanation: