Vendor: Fortinet

Exam Code: FCP_WCS_AD-7.4

Exam Name: FCP - AWS Cloud Security 7.4 Administrator

Version: DEMO

QUESTION 1
Refer to the exhibit. You deployed an active-passive FortiGate HA cluster using a CloudFormation 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.

HA debug output

```
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 port 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-105GGE537X83
awsd get region us-east-2
awsd get vpc id vpc-0e3cf73524e2f8b4e
awsd doing ha failover for vdom root
awsd moving secondary ip for port1
awsd moving secip 10.0.0.13 from eni-0b61d8afc0aefb8a2 to eni-0fe62eb04b2a842e5
awsd move secondary ip successfully
awsd associate elastic ip allocation eipalloc-090425f83f912c8d6 to 10.0.0.13 of eni eni-fe62eb04b2a842e5 awsd associate elastic ip successfully
awsd moving secondary ip for port2 awsd moving secip 10.0.1.13 from eni-0f6b35f8fccd24eb0 to eni-07ec2fadf14bb495d
awsd move secondary ip successfully
awsd update route table rtb-0ae2b70de61129257, replace route of dst 0.0.0.0/0 to eni-07ec2fadf14bb495d
awsd update route successfully
HA state: master
send_vip_arp: vd root master 1 intf port 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-105GGE537X83
awsd get region us-east-2
awsd get vpc id vpc-0e3cf73524e2f8b4e
awsd doing ha failover for vdom root
```

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 10.0.0.13 is now associated with eni-0b61d8afc0aefb8a2.
D. The Elastic IP is associated with port2 of Fgt2, and the secondary IP address for port1 and port2 was updated successfully.

Answer: B
Explanation:
HA Event and Failover:
The debug output indicates that a failover event occurred and the secondary instance (Fgt2) is now taking over as the master.
Elastic IP Association:
The debug output shows the process of moving the Elastic IP (eipalloc-090425f83f912c8d6) to the new master instance. This involves associating the Elastic IP with the appropriate network interface (eni) of the new master.
Specific IP Address Association:
The Elastic IP is specifically associated with port1 of Fgt2. The message "associate elastic ip eipalloc- 090425f83f912c8d6 to 10.0.0.13 of eni eni-0f6b35f8fccd24eb0" indicates that the Elastic IP is now linked to the primary IP address (10.0.0.13) on port1 of the new master.

QUESTION 2
Your customers have been reporting slow response times when accessing your web application. What are two possible ways to increase response times from web servers protected by FortiWeb Cloud? (Choose two.)

A. Deploy FortiWeb Cloud in the same region where your web application is being hosted.

B. Enable a content delivery network (CDN).
C. Modify DNS entries to directly point to your web server.
D. Disable WAF functionality.

Answer: AB
Explanation:
Same Region Deployment:
Deploying FortiWeb Cloud in the same AWS region as your web application minimizes latency and ensures faster response times by reducing the distance data needs to travel (Option A).
Content Delivery Network (CDN):
Enabling a CDN can significantly improve response times by caching content closer to the end-users, reducing the load on the origin server, and speeding up content delivery (Option B).

QUESTION 3
Your company deployed a FortiSandbox for AWS.
Which statement is correct about FortiSandbox for AWS?

A. FortiSandbox for AWS comes as a hybrid solution. The FortiSandbox manager is installed on-premises and analyzes the results of the sandboxing process received from AWS EC2 instances.
B. The FortiSandbox manager is installed on the AWS platform and analyzes the results of the sandboxing process received from on-premises Windows instances.
C. FortiSandbox for AWS does not need more resources because it performs only management and analysis tasks.
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: D
Explanation:
FortiSandbox Deployment:
FortiSandbox for AWS deploys new EC2 instances to create isolated environments where it can safely execute and analyze suspicious files. These instances run custom Windows and Linux virtual machines specifically configured for sandboxing (Option D).
Sandboxing Process:
The process involves sending potential malware to these isolated VMs, executing it, and monitoring its behavior to detect malicious activities. The results are then captured and analyzed to provide detailed threat intelligence.

QUESTION 4
A customer has deployed FortiGate Cloud-Native Firewall (CNF).
Which two statements are correct about policy sets? (Choose two.)

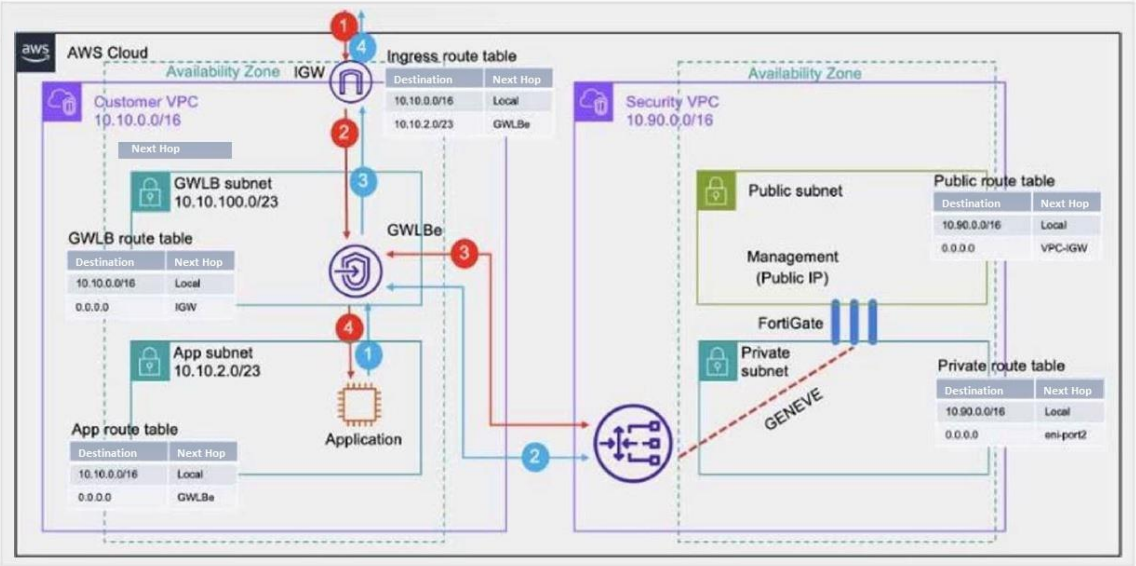
A. There is an implicit deny rule at the bottom of the policy set.
B. The policy set must be manually synchronized to the CNF instance each time it is modified.
C. A new policy set is created with each deployed CNF instance.
D. Multiple policy sets can be applied to a single CNF instance.

Answer: AD
Explanation:
Implicit Deny Rule:
Similar to traditional firewall rule sets, FortiGate Cloud-Native Firewall (CNF) includes an implicit deny rule at the bottom of each policy set. This means any traffic that does not match an existing

rule in the policy set is automatically denied (Option A).
Policy Set Creation:
When a new CNF instance is deployed, a new policy set is created specifically for that instance. This ensures that each CNF instance can have a tailored set of security policies based on the specific needs of the deployment (Option C).

QUESTION 5
Refer to the exhibit. Which two statements are true about inbound traffic based on the IGW ingress route table and GWLB deployment shown in the exhibit? (Choose two.)

GWLB deployment



A. GWLB forwards traffic to FortiGate without encapsulation in its dedicated subnet.
B. Inbound traffic is directed to the GWLB through a GWLB endpoint.
C. Inbound traffic is directed to the application subnet through a GWLB endpoint.
D. GWLB encapsulates traffic with the GENEVE protocol and sends it to FortiGate.

Answer: BD
Explanation:
Traffic Direction through GWLB Endpoint:
The ingress route table directs inbound traffic to the GWLB through a GWLB endpoint (GWLBe). This endpoint is responsible for directing traffic to the Gateway Load Balancer for further processing (Option B).
GENEVE Encapsulation:
The GWLB encapsulates the inbound traffic using the GENEVE protocol. This encapsulated traffic is then sent to FortiGate instances for security inspection. The use of GENEVE ensures that the original traffic context is preserved and can be analyzed by FortiGate (Option D).

QUESTION 6
You are troubleshooting 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 are two reasons for this? (Choose two.)

A. The firewall in the Windows VM is blocking the traffic.
B. The default AWS Network Access Control List (NACL) does not allow this traffic.
C. By default, AWS does not allow ICMP traffic between subnets.
D. Add an inbound allow ICMP rule in the security group attached to the windows server.

Answer: AD
Explanation:
Windows Firewall Blocking Traffic:
The firewall on the Windows VM might be configured to block incoming ICMP traffic (ping requests). By default, Windows Firewall is set to block ICMP traffic, which could be a reason for the connectivity issue (Option A).
Security Group Configuration:
AWS Security Groups act as virtual firewalls for instances. If there is no rule allowing ICMP traffic in the security group attached to the Windows server, the ping requests from FortiGate will be blocked. An inbound allow ICMP rule must be added to the security group to permit this traffic (Option D).

QUESTION 7
An administrator wants to deploy a solution to automatically create firewall rules on FortiGate to accelerate time-to-protection for threats.
Which AWS service can be integrated with FortiGate to accomplish this?

A. AWS Firewall Manager
B. AWS network access control list (NACL)
C. SDN Connector for AWS
D. AWS GuardDuty

Answer: D
Explanation:
AWS GuardDuty Integration:
AWS GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads. It can generate findings that can be used to create or update firewall rules automatically in FortiGate to enhance security and provide timely protection (Option D).
Integration with FortiGate:
GuardDuty findings can be integrated with FortiGate using automation tools and scripts to create firewall rules dynamically, thereby accelerating the time-to-protection against emerging threats.

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**