Fortinet.FCP_WCS_AD-7.4.by.Tom.18q

Number: FCP_WCS_AD-7.4
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: FCP_WCS_AD-7.4

Exam Name: FCP - AWS Cloud Security 7.4 Administrator

Exam A

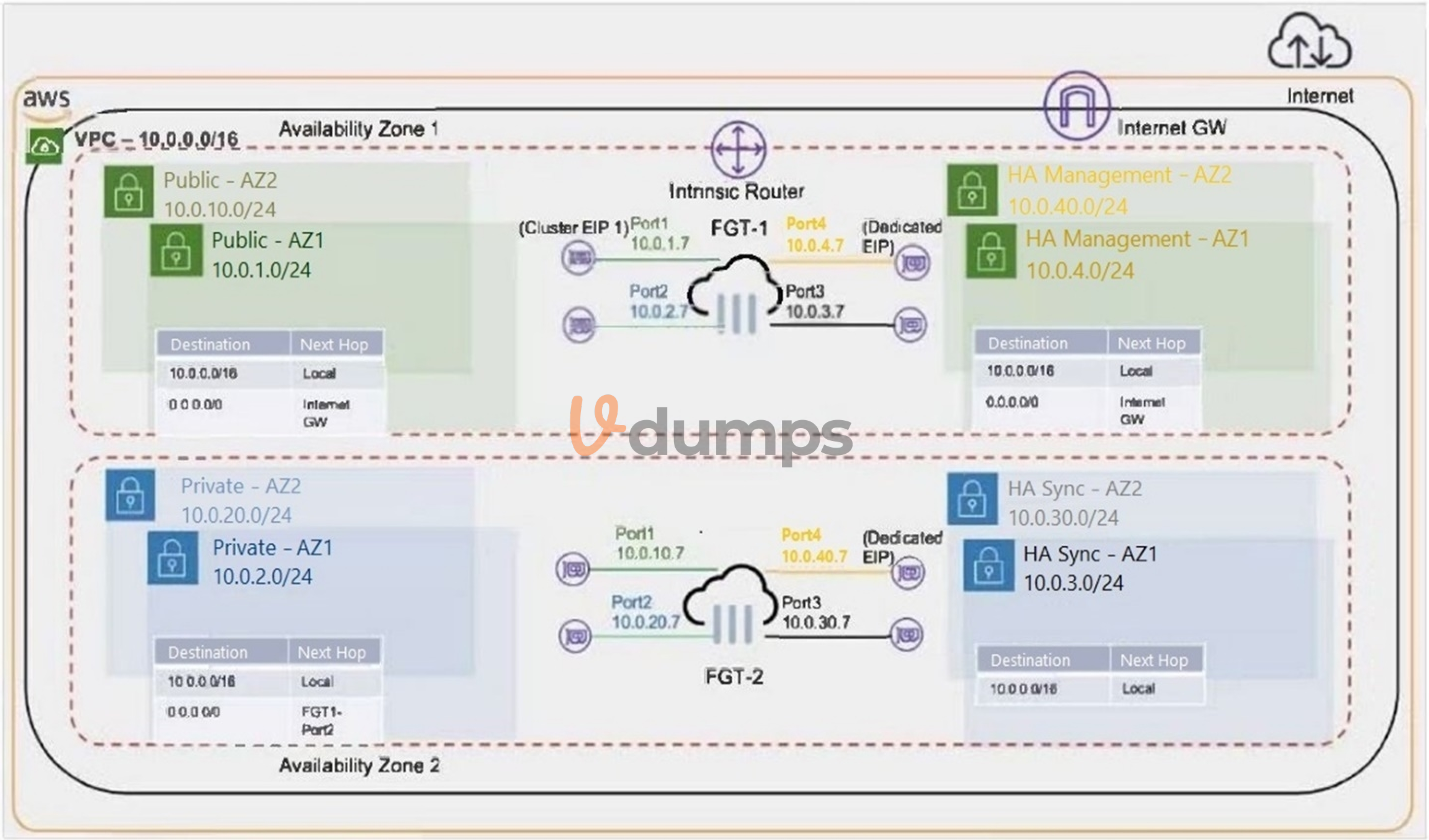
QUESTION 1
A customer is attempting to deploy an active-passive high availability (HA) cluster using the software-defined network (SDN) connector in the AWS cloud.
What is an important consideration to ensure a successful formation of HA, failover, and traffic flow?

A. Both cluster members must be in the same availability zone.
B. VDOM exceptions must be configured.
C. Unicast FortiGate Clustering Protocol (FGCP) must be used.
D. Both cluster members must show as healthy in the elastic load balancer (ELB) configuration.

Correct Answer: C
Section:
Explanation:
HA Cluster in AWS Cloud:
Deploying an active-passive HA cluster in AWS requires careful consideration of the clustering protocol used to ensure seamless failover and traffic flow.
Unicast FortiGate Clustering Protocol (FGCP):
Unicast FGCP is specifically designed for environments where multicast traffic is not feasible or supported, such as in the AWS cloud. Using unicast FGCP ensures that heartbeat and synchronization traffic between the cluster members are managed correctly over unicast communication, which is suitable for AWS's network infrastructure (Option C).
Comparison with Other Options:
Option A is incorrect because while placing both cluster members in the same availability zone might be required for certain configurations, it is not the critical factor for HA formation.
Option B is incorrect as VDOM exceptions are not directly related to the successful formation of HA.
Option D is incorrect because the ELB configuration checks are more about ensuring that the load balancer correctly routes traffic but do not specifically ensure HA formation and failover.
FortiGate HA in AWS Documentation: FortiGate HA
Fortinet FGCP Details: FGCP Documentation

QUESTION 2
Refer to the exhibit.

Active-Passive HA failover



Destination	Next Hop
10.0.0.0/16	Local
0.0.0.0/0	Internet GW

Destination	Next Hop
10.0.0.0/16	Local
0.0.0.0/0	Internet GW

Destination	Next Hop
10.0.0.0/16	Local
0.0.0.0/0	FGT1-Port2

Destination	Next Hop
10.0.0.0/16	Local

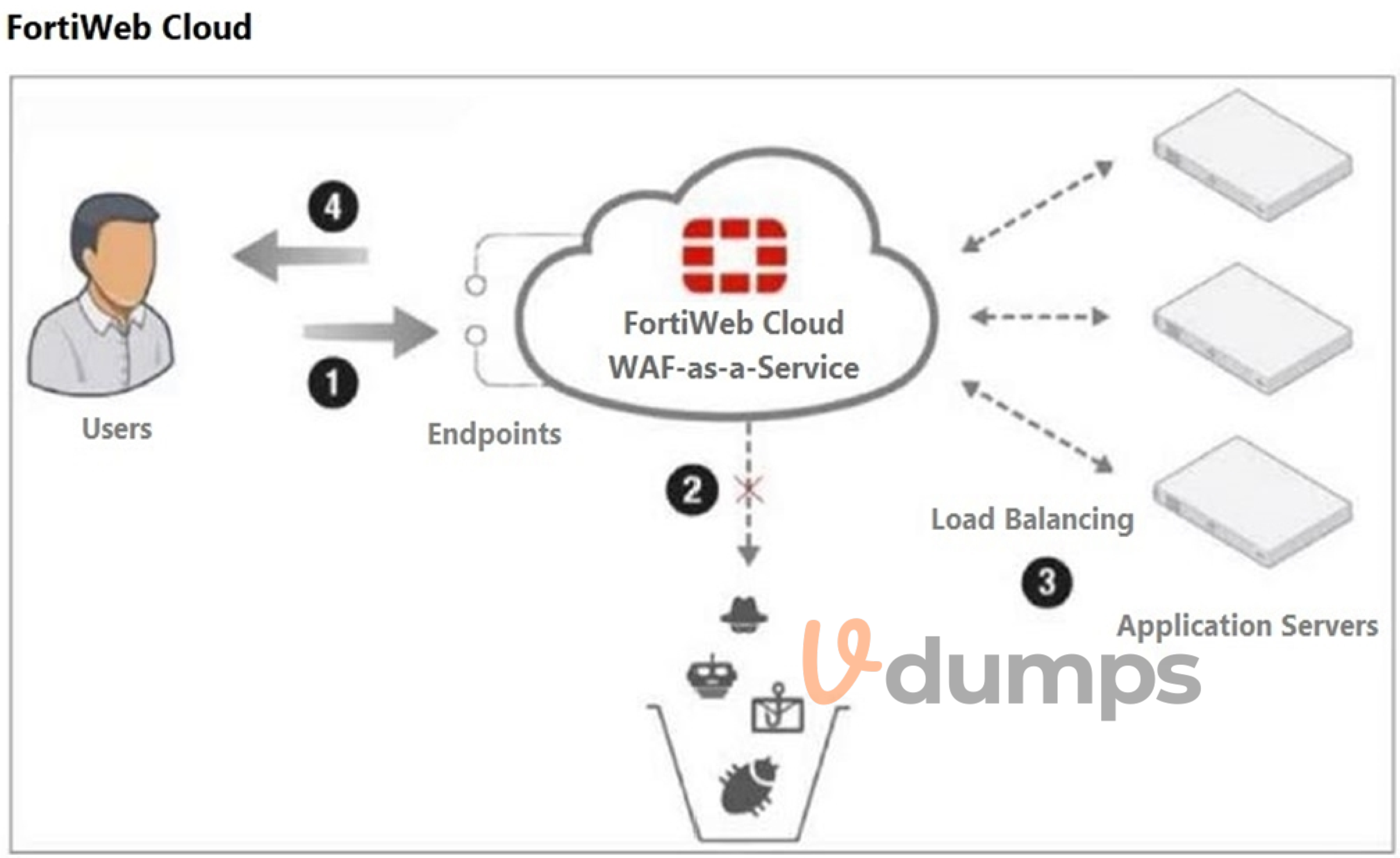
What occurs during a failover for an active-passive (A-P) cluster that is deployed in two different availability zones? (Choose two.)

A. The cluster elastic IP address (EIP) is moved from Port1 of FGT-1 to Port1 of FGT-2.

B. The secondary IP address of Port2 of FGT-1 is moved to Port2 of FGT-2.
C. The default static route in the Private-AZ1 subnet route table is modified to forward all traffic to Port2 of FGT2.
D. An additional route is added to the route table of the HA Sync AZ2 subnet to forward all traffic to the Internet GW.

Correct Answer: A, B
Section:
Explanation:
Cluster Elastic IP Address (EIP) Movement:
During a failover in an active-passive (A-P) cluster, the Elastic IP (EIP) associated with the active FortiGate instance (FGT-1) needs to be moved to the passive instance (FGT-2), which becomes the new active instance. This ensures that the traffic directed to the EIP is now handled by FGT-2 (Option A).
Secondary IP Address Movement:
The secondary IP address on Port2 of the current active instance (FGT-1) is moved to the same port on the new active instance (FGT-2). This step is crucial to ensure seamless network traffic redirection and connectivity for the services relying on that IP address (Option B).
Other Options Analysis:
Option C is incorrect because the static route modification mentioned is not directly related to the failover process described.
Option D is incorrect because no additional route needs to be added to the HA Sync AZ2 subnet route table to forward traffic to the Internet Gateway during a failover.
FortiGate HA Configuration Guide: FortiGate HA
AWS Elastic IP Documentation: Elastic IP

QUESTION 3
Refer to the exhibit.



Which two statements are correct about traffic flow in FortiWeb Cloud? (Choose two.)

A. The DNS name for the application servers must point to FortiWeb Cloud.

B. FortiWeb Cloud filters the incoming traffic from users, blocking the OWASP Top 10 attacks, zero-day threats, and other application layer attacks.

C. FortiWeb Cloud can protect the application servers only if they are all located in the same virtual public cloud (VPC).

D. Step 2 requires an AWS S3 bucket to be created.

Correct Answer: A, B
Section:
Explanation:
DNS Configuration:
For FortiWeb Cloud to effectively protect web applications, the DNS records for the application servers must be configured to point to FortiWeb Cloud. This ensures that all incoming traffic is routed through FortiWeb Cloud for inspection and protection (Option A).
Traffic Filtering:
FortiWeb Cloud provides robust protection by filtering incoming traffic to block the OWASP Top 10 attacks, zero-day threats, and other application layer attacks. This ensures the security and integrity of the web applications it protects (Option B).
Other Options Analysis:

Option C is incorrect because FortiWeb Cloud can protect application servers across different VPCs or regions, not just within the same VPC.
Option D is incorrect because step 2 does not require an AWS S3 bucket; it refers to the inspection and filtering of incoming traffic.
FortiWeb Cloud Overview: FortiWeb Cloud
DNS Configuration for Web Applications: DNS Configuration

QUESTION 4
What is a drawback of deploying a FortiWeb VM inside a virtual public cloud (VPC) compared to FortiWeb Cloud?

A. It is unable to support web applications from OWASP Top 10 threats.
B. It does not support zero-day protection.
C. It is slower than FortiWeb Cloud to apply advanced WAF protection.
D. Only applications going through the VPC are protected.

Correct Answer: D
Section:
Explanation:
VPC-Scoped Protection:
When deploying a FortiWeb VM inside a Virtual Private Cloud (VPC), the security and protection it offers are limited to the applications and traffic that pass through that specific VPC. This means that any applications outside this VPC will not benefit from the protection of FortiWeb VM (Option D).
Comparison with FortiWeb Cloud:
FortiWeb Cloud, being a cloud-native WAF-as-a-Service, can protect applications regardless of their VPC location, offering broader and more flexible protection capabilities.
Other Options Analysis:
Option A is incorrect because both FortiWeb VM and FortiWeb Cloud protect against OWASP Top 10 threats.
Option B is incorrect because FortiWeb VM does support zero-day protection.
Option C is incorrect as the performance of FortiWeb VM in applying advanced WAF protection is not inherently slower compared to FortiWeb Cloud.
FortiWeb Overview: FortiWeb

QUESTION 5
An AWS administrator is designing internet connectivity for an organization's virtual public cloud (VPC). The organization has web servers with private addresses that must be reachable from the internet. The web servers must be highly available.
Which two configurations can you use to ensure the web servers are highly available and reachable from the internet? (Choose two.)

A. Deploy a network load balancer.
B. Configure a network address translation (NAT) Gateway in your VPC. Place web servers behind the NAT Gateway.
C. Add a route to the default virtual public cloud (VPC) route table forwarding all traffic to the internet gateway.
D. Deploy web servers in multiple availability zones.

Correct Answer: A, D
Section:
Explanation:
Network Load Balancer:
Deploying a network load balancer ensures that incoming traffic is distributed across multiple web servers, providing high availability and redundancy. This setup helps in managing traffic efficiently and maintaining service uptime even if some servers fail (Option A).
Multiple Availability Zones:
Deploying web servers in multiple availability zones (AZs) enhances fault tolerance and availability. If one AZ goes down, servers in other AZs can continue to handle the traffic, ensuring the web application remains accessible (Option D).
Other Options Analysis:
Option B is incorrect because NAT Gateways are used to provide internet access to instances in private subnets, not to make private addresses reachable from the internet.
Option C is not sufficient on its own for high availability. Adding a route to the default VPC route table forwarding traffic to the internet gateway makes the VPC internet-accessible but does not ensure high availability.

AWS High Availability and Fault Tolerance: AWS High Availability
AWS Network Load Balancer: Network Load Balancer

QUESTION 6
A cloud administrator is tasked with protecting web applications hosted in AWS cloud.
Which three Fortinet cloud offerings can the administrator choose from to accomplish the task? (Choose three.)

A. AWS WAF
B. FortiEDR
C. FortiGate Cloud-Native Firewall (CNF)
D. Fortinet Managed Rules for AWS WAF
E. FortiWeb Cloud

Correct Answer: C, D, E
Section:
Explanation:
FortiGate Cloud-Native Firewall (CNF):
FortiGate CNF offers cloud-native firewall capabilities designed to provide network security within AWS. It integrates seamlessly with AWS services and offers advanced threat protection and traffic management (Option C).
Fortinet Managed Rules for AWS WAF:
Fortinet Managed Rules for AWS WAF provide pre-configured, updated security rules that protect web applications from common threats such as SQL injection and cross-site scripting. This offering simplifies the protection of web applications hosted on AWS (Option D).
FortiWeb Cloud:
FortiWeb Cloud is a Web Application Firewall (WAF) as a service that provides comprehensive protection for web applications hosted on AWS. It offers features such as bot mitigation, DDoS protection, and deep inspection of HTTP/HTTPS traffic (Option E).
Comparison with Other Options:
Option A (AWS WAF) is a native AWS service, not a Fortinet offering.
Option B (FortiEDR) is focused on endpoint detection and response, which is not specifically aimed at protecting web applications.
FortiGate CNF Documentation: FortiGate CNF
Fortinet Managed Rules for AWS WAF: Fortinet AWS WAF Rules
FortiWeb Cloud Overview: FortiWeb Cloud

QUESTION 7
Your organization is deciding between deploying FortiWeb VM or Fortinet Managed Rules for AWS WAF.
What are two benefits of choosing FortiWeb VM? (Choose two.)

A. Only pay for what is used.
B. Up-to-date WAF signatures powered by FortiGuard.
C. Zero-day protection.
D. Advanced WAF functionality.

Correct Answer: C, D
Section:
Explanation:
Zero-day Protection:
FortiWeb VM provides robust protection against zero-day vulnerabilities through advanced security mechanisms and frequent updates from FortiGuard. This ensures that web applications are protected from newly discovered threats that have not yet been patched or recognized by other security systems (Option C).
Advanced WAF Functionality:
FortiWeb VM offers a range of advanced WAF features that go beyond what is typically provided by managed rules for AWS WAF. These include more detailed traffic analysis, customizable rules, machine learning-based threat

detection, and comprehensive logging and reporting capabilities (Option D).
Other Options Analysis:
Option A is more relevant to a consumption-based pricing model but not a specific benefit unique to FortiWeb VM over AWS WAF.
Option B is incorrect because both FortiWeb VM and Fortinet Managed Rules for AWS WAF are powered by FortiGuard updates.
FortiWeb Overview: FortiWeb VM
AWS WAF and Fortinet Managed Rules: AWS WAF

QUESTION 8
You need to deploy a new Windows server in AWS to offload web traffic from an existing web server in a different availability zone.
According to the AWS shared responsibility model, what three actions must you take to secure the new EC2 instance? (Choose three.)

A. Update software on the instance.
B. Change the existing elastic load balancer (ELB) to a gateway load balancer
C. Configure security groups.
D. Manage the operating system on the instance.
E. Move all web servers into the same availability zone.

Correct Answer: A, C, D
Section:
Explanation:
Update Software:
As part of the AWS shared responsibility model, it is the customer's responsibility to update and maintain the software running on the EC2 instance, including applying security patches and updates (Option A).
Configure Security Groups:
Security groups act as virtual firewalls for instances to control inbound and outbound traffic. Configuring them correctly is essential for securing the EC2 instance and ensuring only legitimate traffic can reach the server (Option C).
Manage Operating System:
Managing the operating system, including user accounts, permissions, and operating system patches, is the responsibility of the customer under the shared responsibility model (Option D).
Other Options Analysis:
Option B is incorrect as changing the existing ELB to a gateway load balancer is not necessary for securing the new EC2 instance.
Option E is incorrect because it is not required to move all web servers into the same availability zone for security purposes.
AWS Shared Responsibility Model: AWS Shared Responsibility
EC2 Security Best Practices: AWS EC2 Security

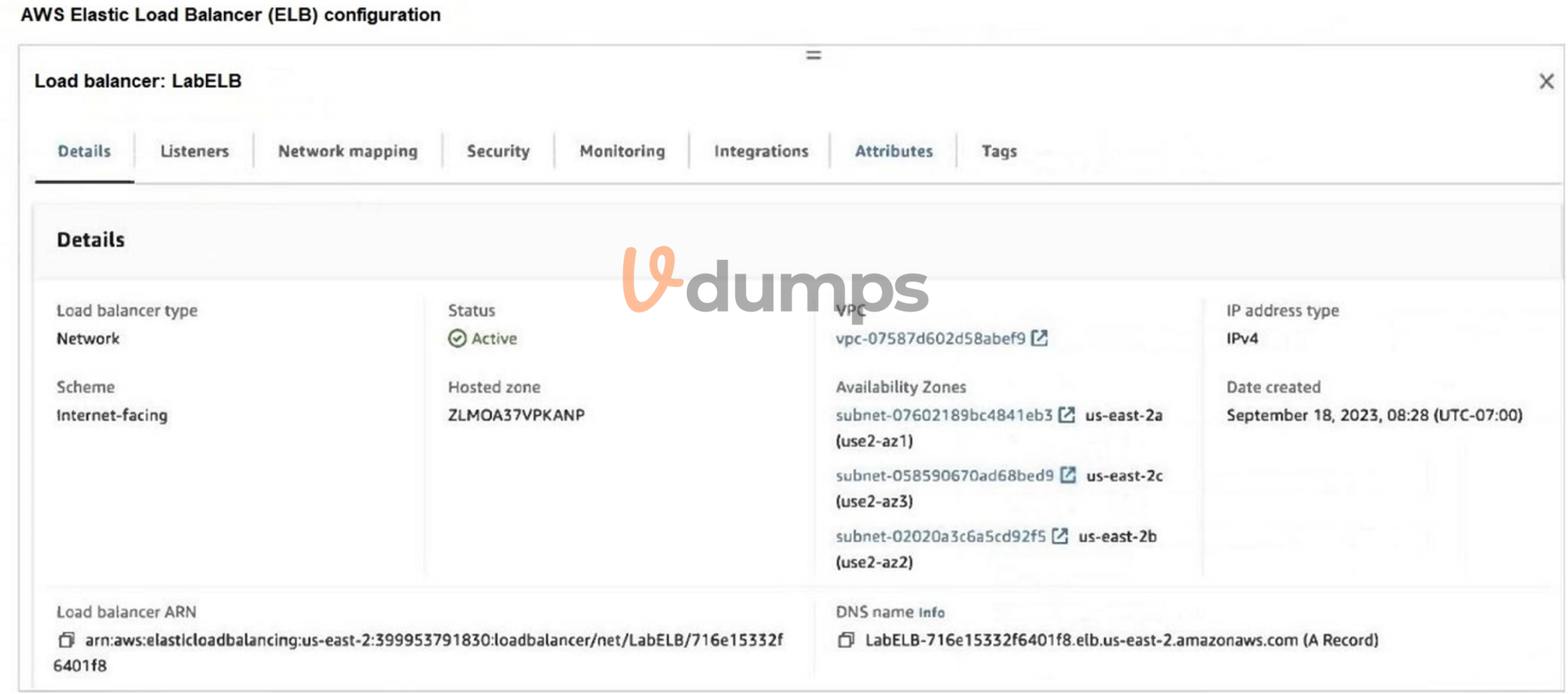
QUESTION 9
An administrator wants to deploy a solution to automatically create firewall rules on FortiGate to accelerate time-to-protection for threats.
Which AWS service can be integrated with FortiGate to accomplish this?

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

Correct Answer: D
Section:
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.
Other Options Analysis:
Option A (AWS Firewall Manager) is more suited for managing rules across multiple accounts but not for dynamic threat response.
Option B (AWS Network ACL) provides stateless filtering but does not offer automated rule creation.
Option C (SDN Connector for AWS) helps in integrating SDN capabilities but is not specifically focused on threat-based rule automation.
AWS GuardDuty: AWS GuardDuty
FortiGate Integration: Fortinet Integration

QUESTION 10
Refer to the exhibit.



AWS Elastic Load Balancer (ELB) configuration

Load balancer: LabELB

Details

Load balancer type
Network

Status
Active

VPC
vpc-07587d602d58abef9

IP address type
IPv4

Scheme
Internet-facing

Hosted zone
ZLMOA37VPKANP

Availability Zones
subnet-07602189bc4841eb3 us-east-2a (use2-az1)
subnet-058590670ad68bed9 us-east-2c (use2-az3)
subnet-02020a3c6a5cd92f5 us-east-2b (use2-az2)

Date created
September 18, 2023, 08:28 (UTC-07:00)

Load balancer ARN
arn:aws:elasticloadbalancing:us-east-2:399953791830:loadbalancer/net/LabELB/716e15332f6401f8

DNS name Info
LabELB-716e15332f6401f8.elb.us-east-2.amazonaws.com (A Record)

A customer is using the AWS Elastic Load Balancer (ELB).
Which two statements are correct about the ELB configuration? (Choose two.)

A. The load balancer is configured to load balance traffic among multiple availability zones.
B. The Amazon Resource Name is used to access the load balancer node and targets.

C. You can use the DNS name to reach the targets behind the ELB.
D. The load balancer is configured for the internal traffic of the virtual public cloud (VPC).

Correct Answer: A, C
Section:
Explanation:
Load Balancer Configuration Overview:
The provided configuration indicates that the ELB is an internet-facing load balancer.
Multi-AZ Load Balancing:
The load balancer is configured to distribute traffic across multiple availability zones (A, B, and C), ensuring high availability and fault tolerance (Option A).
Accessing Targets via DNS:
The DNS name of the load balancer (LabELB-716e15332f6401f8.elb.us-east-2.amazonaws.com) can be used to reach the targets behind the ELB, facilitating traffic routing to the appropriate instances (Option C).
Comparison with Other Options:
Option B is incorrect as the ARN is not used to access the load balancer directly.
Option D is incorrect because the load balancer is configured for internet-facing traffic, not just internal VPC traffic.
AWS Elastic Load Balancer Documentation: AWS ELB
Understanding ELB DNS: AWS ELB DNS

QUESTION 11
Which two statements about the FortiCloud portal are true? (Choose two.)

A. You can gain remote access to your FortiGate VM directly from the portal.
B. To assign permissions in the identity and access management (JAM) portal, you must write a JSON script.
C. You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare.
D. You can access only cloud services that you have subscribed to on AWS marketplace.

Correct Answer: A, C
Section:
Explanation:
Remote Access to FortiGate VM:
The FortiCloud portal allows users to remotely access their FortiGate VM instances. This is particularly useful for managing and configuring instances without needing direct network access (Option A).
FortiFlex Portal Access:
The FortiFlex portal is a feature that becomes available only after purchasing a FortiFlex license and registering it on FortiCare. This portal provides additional functionalities and services related to FortiFlex (Option C).
IAM Permissions:
Option B is incorrect because the Identity and Access Management (IAM) permissions in the FortiCloud portal do not require writing JSON scripts; they can be managed through the portal interface.
Subscription to Cloud Services:
Option D is incorrect because FortiCloud provides access to services beyond those subscribed through the AWS marketplace, including services directly offered by Fortinet.
FortiCloud Documentation: FortiCloud
FortiFlex Portal: FortiFlex Licensing

QUESTION 12
Which three statements are correct about VPC flow logs? (Choose three.)

A. Flow logs do not capture traffic to and from 169.254.169.254 for instance metadata.
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 can capture real-time log streams for the network interfaces.

Correct Answer: A, B, D
Section:
Explanation:
Instance Metadata Traffic:
VPC flow logs do not capture traffic to and from the link-local address 169.254.169.254, which is used for accessing instance metadata (Option A).
DHCP Traffic:
DHCP traffic is not captured by VPC flow logs. This is because DHCP relies on broadcast and multicast traffic, which is excluded from flow logs (Option B).
Security Monitoring:
VPC flow logs can be used as a security tool to monitor the traffic that is reaching the instances. By analyzing the flow logs, administrators can detect suspicious activities and troubleshoot connectivity issues (Option D).
Other Considerations:
Option C is incorrect because flow logs do capture traffic to the reserved IP address of the default VPC router.
Option E is incorrect as VPC flow logs do not provide real-time log streams but rather capture data at intervals and deliver them to CloudWatch or S3.
AWS VPC Flow Logs Documentation: VPC Flow Logs
AWS Networking and Security: AWS Security Monitoring

QUESTION 13
An administrator is adding a web application to be protected by FortiWeb Cloud.
Which two steps are necessary to successfully onboard the application? (Choose two.)
An administrator is adding a web application to be protected by FortiWeb Cloud.
Which two steps are necessary to successfully onboard the application? (Choose two.)

A. Wait for the EC2 instance to be created.
B. Provide a web application name.
C. Create DNS records in the domain server that hosts the application.
D. Enable a content delivery network (CDN) in the same region where your application is located.

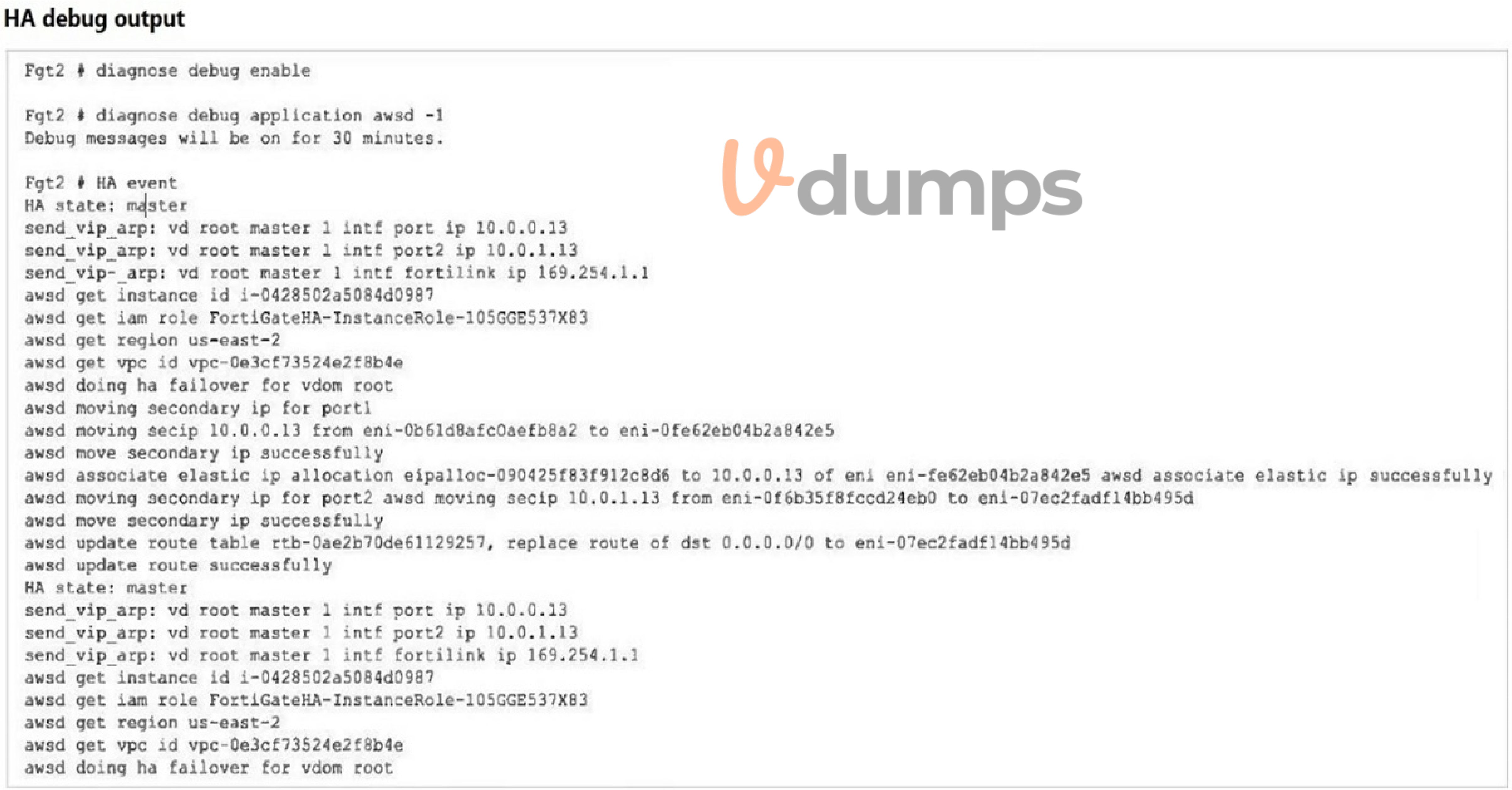
Correct Answer: B, C
Section:
Explanation:
Web Application Name:
When onboarding a web application to be protected by FortiWeb Cloud, you need to provide a name for the web application. This helps in identifying and managing the application within the FortiWeb Cloud console (Option B).
DNS Records:
To ensure that traffic to your web application is correctly routed through FortiWeb Cloud, you must create DNS records in the domain server that hosts your application. This ensures that requests are directed to FortiWeb Cloud for inspection and protection (Option C).
Other Considerations:
Option A (Waiting for the EC2 instance) is incorrect as it is not a necessary step for onboarding a web application to FortiWeb Cloud.
Option D (Enabling a CDN) is not a mandatory step for onboarding but can be part of a broader strategy for improving performance and protection.
FortiWeb Cloud Documentation: FortiWeb Cloud

QUESTION 14
An administrator must deploy a web application firewall (WAF) solution to protect the web applications of their organization.
Why would the administrator choose FortiWeb Cloud over AWS WAF with Fortinet managed rules?

A. WAF signatures must be manually updated by FortiGuard.
B. The solution must meet PCI 6.6 compliance.
C. SSL inspection is a requirement.
D. Traffic must be inspected for malware.

Correct Answer: C
Section:
Explanation:
SSL Inspection Requirement:
FortiWeb Cloud provides comprehensive SSL inspection capabilities, allowing it to decrypt and inspect HTTPS traffic for threats. This is a crucial feature for many organizations that need to ensure all traffic, including encrypted traffic, is thoroughly inspected (Option C).
Comparison with AWS WAF:
While AWS WAF with Fortinet managed rules provides robust protection, it might not offer the same level of SSL inspection capabilities as FortiWeb Cloud.
Other Considerations:
Option A (Manual WAF signature updates) is incorrect because FortiWeb Cloud updates signatures automatically.
Option B (PCI 6.6 compliance) is a general requirement for any WAF solution, not specific to choosing FortiWeb Cloud over AWS WAF.
Option D (Traffic inspection for malware) is a feature provided by both FortiWeb Cloud and AWS WAF with Fortinet managed rules.
FortiWeb Cloud Overview: FortiWeb Cloud
AWS WAF Documentation: AWS WAF

QUESTION 15
Refer to the exhibit.



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
```

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.
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.

Correct Answer: B
Section:
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.
Other Options Analysis:
Option A is incorrect because the routing table update details are not explicitly stated.
Option C is incorrect because the IP address association mentioned relates to an Elastic IP, not eni-0b61d8afc0aefb8a2.
Option D is incorrect because it specifically mentions port2 for the Elastic IP association, which is not indicated in the debug output.
FortiGate HA Configuration Guide: FortiGate HA
AWS Elastic IP Documentation: Elastic IP

QUESTION 16
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.)
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
C. Modify DNS entries to directly point to your web server.
D. Disable WAF functionality.

Correct Answer: A, B
Section:
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).
Other Options Analysis:
Option C is incorrect because modifying DNS entries to directly point to your web server bypasses the WAF protection, which is not advisable for security reasons.
Option D is incorrect because disabling WAF functionality would expose your web application to vulnerabilities and threats, compromising security.
AWS Regions and Availability Zones: AWS Regions
Content Delivery Network Overview: AWS CloudFront

QUESTION 17
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.

Correct Answer: D
Section:
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.
Other Options Analysis:
Option A is incorrect because FortiSandbox for AWS operates entirely within the AWS environment and does not require an on-premises manager.
Option B is incorrect as the FortiSandbox manager is not installed on the AWS platform for managing on-premises instances.
Option C is incorrect because FortiSandbox requires sufficient resources to perform the actual sandboxing and analysis tasks.
FortiSandbox for AWS Documentation: FortiSandbox
Sandboxing Concepts: Sandboxing

QUESTION 18
An administrator needs to attach an Elastic Network Interface (ENI) to an application instance in a VPC with multiple availability zones. An instance runs in availability zone 1.
Which ENI property must the administrator consider when implementing this requirement?

A. An ENI cannot attach to an instance in availability zone 2.
B. After the ENI detaches from one instance, it can reattach only to the same instance.
C. You can detach the primary ENI from an AWS instance.
D. When you move an ENI, network traffic remains directed to the old instance until you terminate that instance.

Correct Answer: A
Section:
Explanation:
ENI Attachment Across Availability Zones:
Elastic Network Interfaces (ENIs) are associated with a specific Availability Zone. They cannot be attached to instances that are in a different Availability Zone than where the ENI was created. Therefore, an ENI created in Availability Zone 1 cannot be attached to an instance in Availability Zone 2 (Option A).
ENI Reattachment:
ENIs can be detached from one instance and reattached to another instance within the same Availability Zone. This flexibility allows for network interface configuration to be preserved across instance changes within the same AZ.
Other Options Analysis:
Option B is incorrect because an ENI can be reattached to any instance in the same AZ.
Option C is incorrect as the primary ENI (eth0) cannot be detached from an instance.
Option D is incorrect because when an ENI is moved, the traffic is directed to the new instance, and there is no redirection to the old instance.
AWS ENI Documentation: Elastic Network Interfaces
AWS Networking Best Practices: AWS Networking