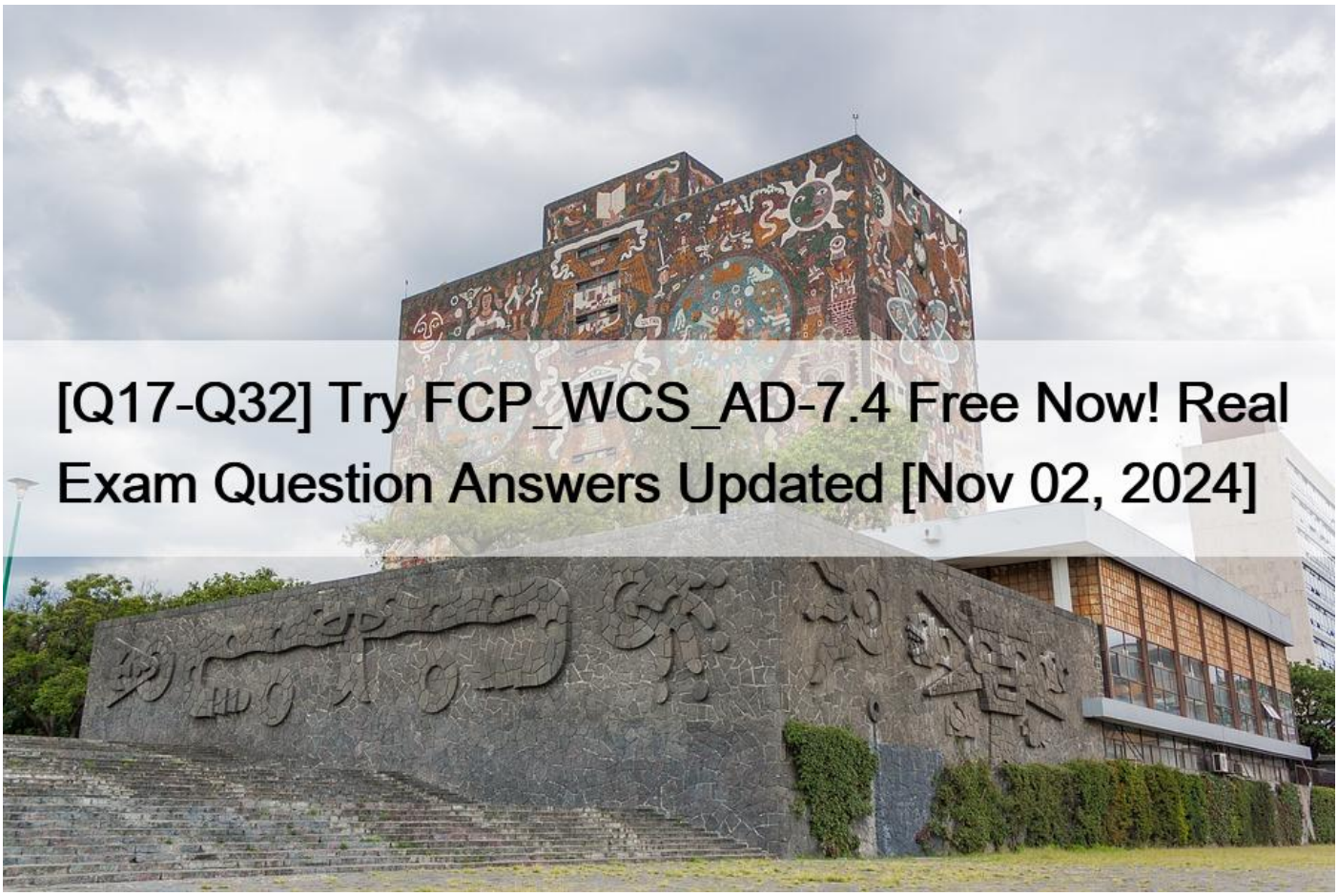
[Q17-Q32 Try FCP_WCS_AD-7.4 Free Now! Real Exam Question Answers Updated [Nov 02, 2024



Try FCP_WCS_AD-7.4 Free Now! Real Exam Question Answers Updated [Nov 02, 2024 Get Ready to Pass the FCP_WCS_AD-7.4 exam with Fortinet Latest Practice Exam

Fortinet FCP_WCS_AD-7.4 Exam Syllabus Topics:

TopicDetailsTopic 1- Fortinet product deployment: Integration of Fortinet solutions in AWS is discussed in this topic. Additionally, the topic focuses on the deployment of WAF in AWS.Topic 2- Load balancers and FortiCNF: Its sub-topics discuss comparing load balancer types in AWS and deploying FortiGate CNF.Topic 3- High availability: It covers the deployment of HA in AWS. Moreover, the topic discusses the configuration of HA by using Fortinet CloudFormation templates.Topic 4- Public cloud fundamentals: It delves into AWS public cloud concepts. Moreover, the topic points out different Fortinet solutions to secure the cloud.Topic 5- AWS components: The topic identifies AWS networking components. It discusses the application of AWS security components. Lastly, the topic describes traffic flow in AWS.

QUESTION 17

An organization has created a VPC with two subnets and deployed a FortiGate-VM (VM04/c4.xlarge) in AWS.

The EC2 instance is initially configured with two Elastic Network Interfaces (ENIs). The primary ENI is configured on the public subnet, and the secondary ENI is configured on the private subnet. To provide internet access for the FortiGate-VM, they now want to associate an EIP to its primary ENI, but the assignment is failing.

Which action would allow the EIP assignment to be successful?
* Create and associate a public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
* Create and attach a public routing table to the public subnet, associate the public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
* Shut down the FortiGate VM, if it is running, assign the EIP to the primary ENI, and then power it on.
* Create and attach an internet gateway to the VPC, and then assign the EIP to the primary ENI of the FortiGate VM.

QUESTION 18

Which two statements about the FortiCloud portal are true? (Choose two.)
* You can gain remote access to your FortiGate VM directly from the portal.
* To assign permissions in the identity and access management (JAM) portal, you must write a JSON script.
* You can access the FortiFlex portal only after you purchase a FortiFlex license and register it on FortiCare.
* You can access only cloud services that you have subscribed to on AWS marketplace.

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.

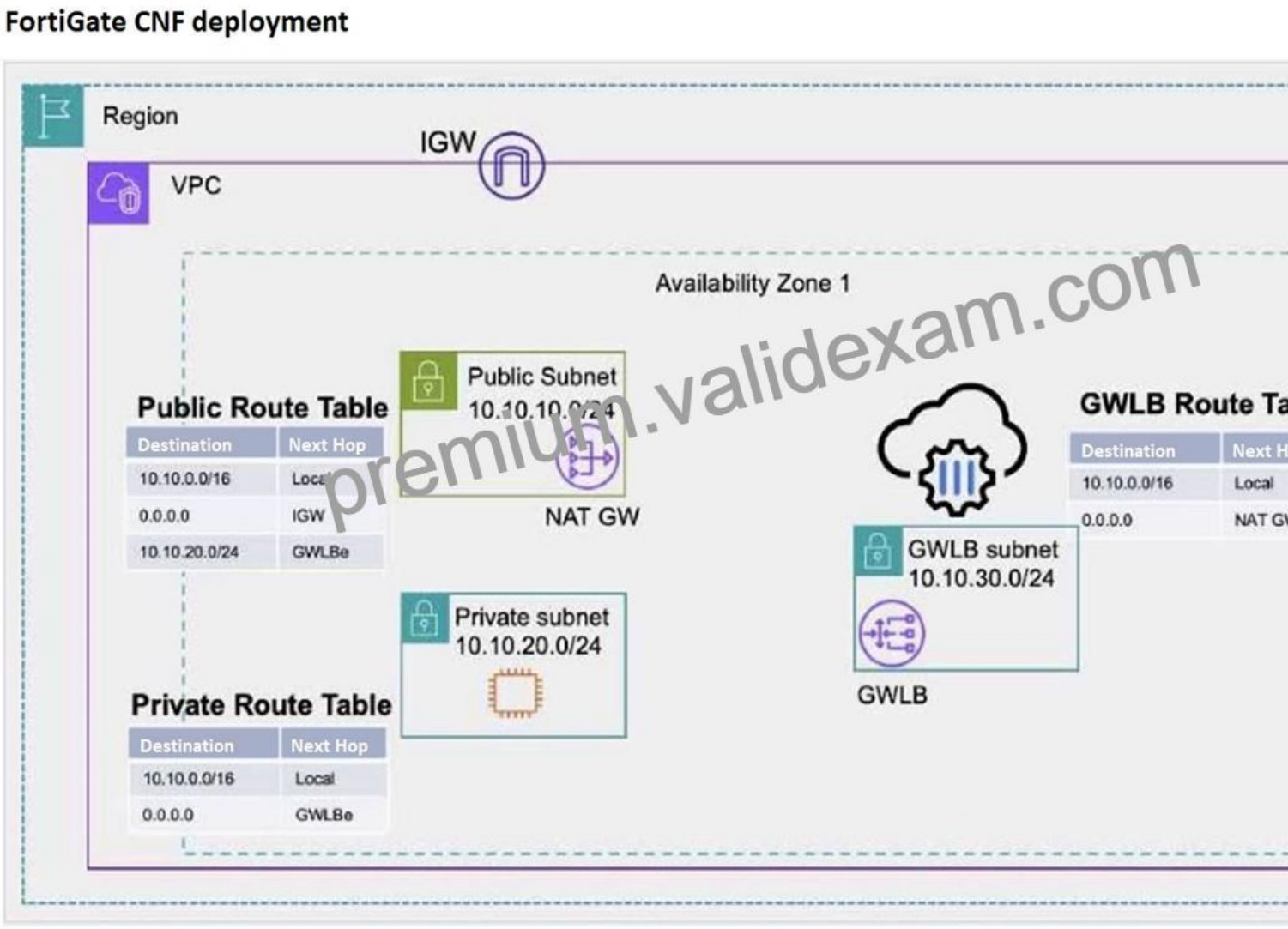
Reference:

FortiCloud Documentation: FortiCloud

FortiFlex Portal: FortiFlex Licensing

QUESTION 19

Refer to the exhibit.



Traffic is initiated from the EC2 instance and is destined for the internet.

Which traffic flow is correct?
* EC2 instance > NAT GW > IGW > internet
* There is no route to the internet in the Private Route Table. The traffic does not reach the internet.
* EC2 instance > GWLBe > NAT GW > IGW > internet
* EC2 instance > GWLBe > internet

Understanding the Architecture:

The architecture includes an EC2 instance in a private subnet, a Gateway Load Balancer Endpoint (GWLBe), a NAT Gateway (NAT GW), and an Internet Gateway (IGW).

Route Tables and Routing:

The private route table for the subnet containing the EC2 instance has a route pointing to the GWLBe for internet-bound traffic.

The public route table for the subnet containing the NAT Gateway has routes to the IGW.

Traffic Flow Analysis:

Traffic initiated from the EC2 instance destined for the internet will first be routed to the GWLBe as per the private route table.

The GWLBe will forward the traffic to the NAT Gateway.

The NAT Gateway will then route the traffic to the IGW, which finally sends the traffic to the internet.

Comparison with Other Options:

Option A suggests direct routing to the NAT GW from the EC2 instance, which is incorrect.

Option B incorrectly states there is no route to the internet in the private route table.

Option D suggests direct routing from GWLBe to the internet, which is not the case.

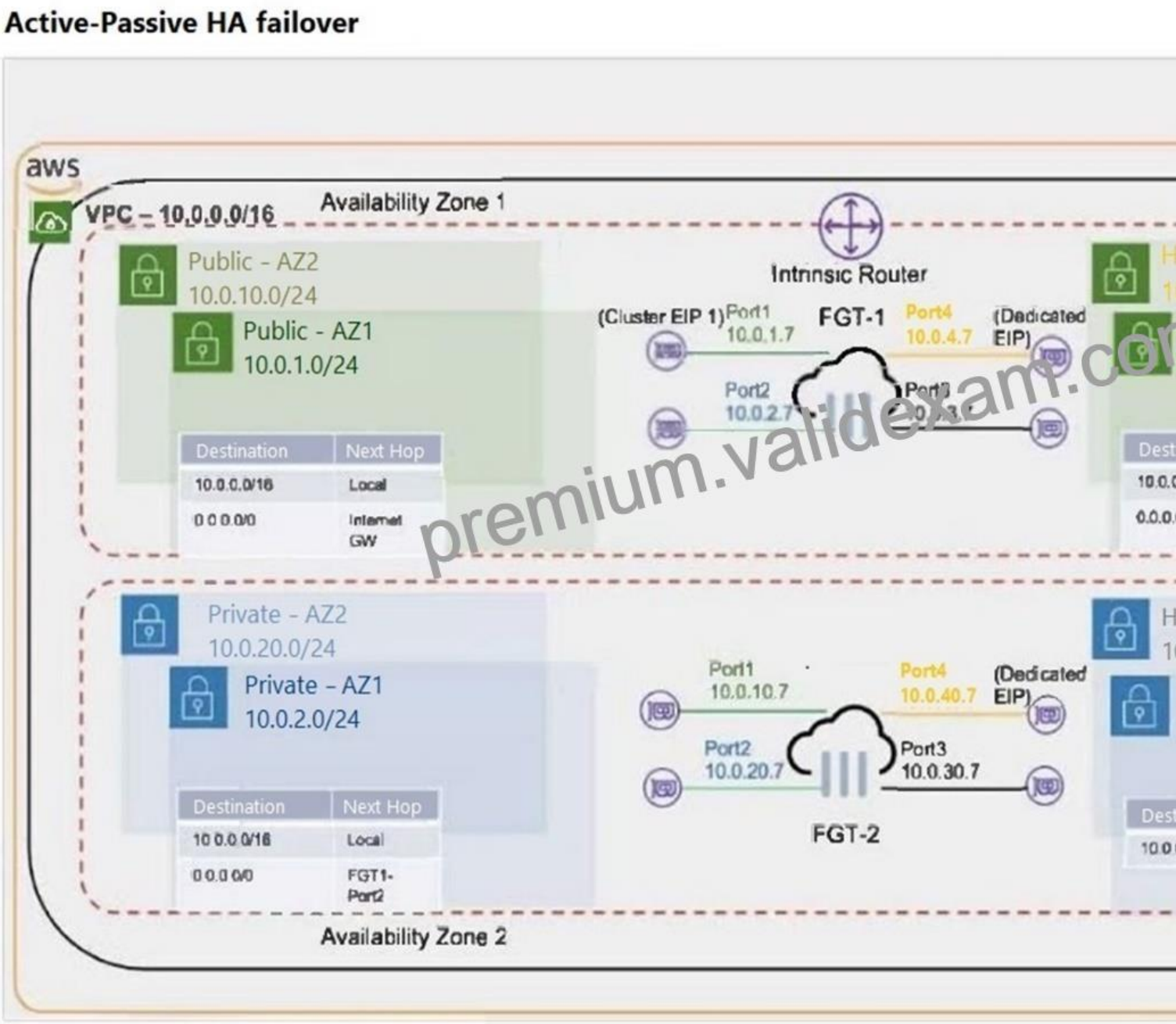
Reference:

AWS Documentation on Route Tables: AWS Route Tables

Gateway Load Balancer Overview: AWS Gateway Load Balancer

QUESTION 20

Refer to the exhibit.



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

* The cluster elastic IP address (EIP) is moved from Port1 of FGT-1 to Port1 of FGT-2.
* The secondary IP address of Port2 of FGT-1 is moved to Port2 of FGT-2.
* The default static route in the Private-AZ1 subnet route table is modified to forward all traffic to Port2 of FGT2.
* An additional route is added to the route table of the HA Sync AZ2 subnet to forward all traffic to the Internet GW.

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.

Reference:

FortiGate HA Configuration Guide: FortiGate HA

AWS Elastic IP Documentation: Elastic IP

QUESTION 21

A customer has deployed FortiGate Cloud-Native Firewall (CNF).

Which two statements are correct about policy sets? (Choose two.)
* There is an implicit deny rule at the bottom of the policy set.
* The policy set must be manually synchronized to the CNF instance each time it is modified.
* A new policy set is created with each deployed CNF instance.
* Multiple policy sets can be applied to a single CNF instance.

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).

Other Options Analysis:

Option B is incorrect because policy sets do not require manual synchronization; they are applied automatically once configured.

Option D is incorrect as a single CNF instance operates with a single policy set at a time.

Reference:

FortiGate CNF Documentation: FortiGate CNF

Firewall Policy Best Practices: Fortinet Policies

QUESTION 22

A customer has implemented GWLB between the partner and application VPCs. FortiGate appliances are deployed in the partner VPC with multiple AZs to inspect traffic transparently.

Which two things will happen to application traffic based on the GWLB deployment? (Choose two.)
* Inbound and outbound traffic will go to multiple devices, which will perform load balancing.
* Inbound and outbound traffic will go to the same device, which will perform stateful processing.
* The content of the original traffic exchanged between the GWLB and FortiGate will be preserved.
* The original traffic exchanged between the GWLB and FortiGate will be hashed for data integrity.

Understanding Gateway Load Balancer (GWLB):

GWLB is designed to distribute traffic across multiple appliances for both inbound and outbound traffic, providing scalability and high availability.

Traffic Load Balancing:

GWLB can send traffic to multiple FortiGate appliances for load balancing purposes, ensuring efficient use of resources (Option A).

Stateful Processing:

For stateful processing, GWLB ensures that traffic flows (both inbound and outbound) for a given connection are directed to the same FortiGate appliance. This maintains session integrity (Option B).

Preservation and Hashing of Traffic:

Options C and D are incorrect as they suggest incorrect behavior regarding traffic content preservation and hashing for data integrity, which are not primary functions of GWLB.

Reference:

AWS Gateway Load Balancer Documentation: AWS Gateway Load Balancer

FortiGate Integration with GWLB: Fortinet Documentation

QUESTION 23

An organization has the requirement to connect a data VPC to the on-premises infrastructure of a branch office in a hybrid cloud environment. The connectivity needs the higher bandwidth but the organization does not want to use multiple connections between sites.

Which AWS solution meets the requirement?
* Transit VPC with IPSec
* Internet Gateway
* Transit Gateway multicast
* Transit Gateway Connect

Understanding the Requirement:

The organization needs to connect a data VPC to the on-premises infrastructure with high bandwidth.

The solution should avoid multiple connections between sites.

Transit Gateway Connect:

Transit Gateway Connect is designed to integrate with SD-WAN networks and provides scalable bandwidth using GRE tunnels.

It simplifies hybrid cloud connectivity by allowing high bandwidth connections without the need for multiple physical connections.

Benefits of Transit Gateway Connect:

Supports scalable bandwidth through GRE tunnels.

Facilitates seamless integration with on-premises and cloud environments.

Reduces complexity by avoiding the need for multiple VPN connections.

Comparison with Other Options:

Option A (Transit VPC with IPSec) is not preferred due to complexity and potential limitations in bandwidth scalability.

Option B (Internet Gateway) is not suitable for private, high-bandwidth connections.

Option C (Transit Gateway multicast) does not address the requirement for high bandwidth in a hybrid cloud setup.

Reference:

AWS Transit Gateway Documentation: AWS Transit Gateway Connect

Hybrid Cloud Connectivity: AWS Hybrid Cloud

QUESTION 24

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.)
* Only pay for what is used.
* Up-to-date WAF signatures powered by FortiGuard.
* Zero-day protection.
* Advanced WAF functionality.

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.

Reference:

FortiWeb Overview: FortiWeb VM

AWS WAF and Fortinet Managed Rules: AWS WAF

QUESTION 25

An organization has created a VPC with two subnets and deployed a FortiGate-VM (VM04/c4.xlarge) in AWS.

The EC2 instance is initially configured with two Elastic Network Interfaces (ENIs). The primary ENI is configured on the public subnet, and the secondary ENI is configured on the private subnet. To provide internet access for the FortiGate-VM, they now want to associate an EIP to its primary ENI, but the assignment is failing.

Which action would allow the EIP assignment to be successful?
* Create and associate a public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
* Shut down the FortiGate VM, if it is running, assign the EIP to the primary ENI, and then power it on.
* Create and attach an internet gateway to the VPC, and then assign the EIP to the primary ENI of the FortiGate VM.
* Create and attach a public routing table to the public subnet, associate the public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.

Internet Gateway Requirement:

For an Elastic IP (EIP) to be assigned to an instance’s primary ENI, the VPC must have an Internet Gateway (IGW) attached. The IGW enables the VPC to communicate with the internet, allowing the EIP to function properly (Option C).

Process of Assigning EIP:

Once the Internet Gateway is attached to the VPC, the EIP can be successfully assigned to the primary ENI of the FortiGate VM, providing it with internet access.

Other Options Analysis:

Option A is incorrect because the primary ENI is already in a public subnet.

Option B is not necessary and may not solve the issue without an attached Internet Gateway.

Option D is partially correct about the routing table but does not address the primary issue of needing an Internet Gateway.

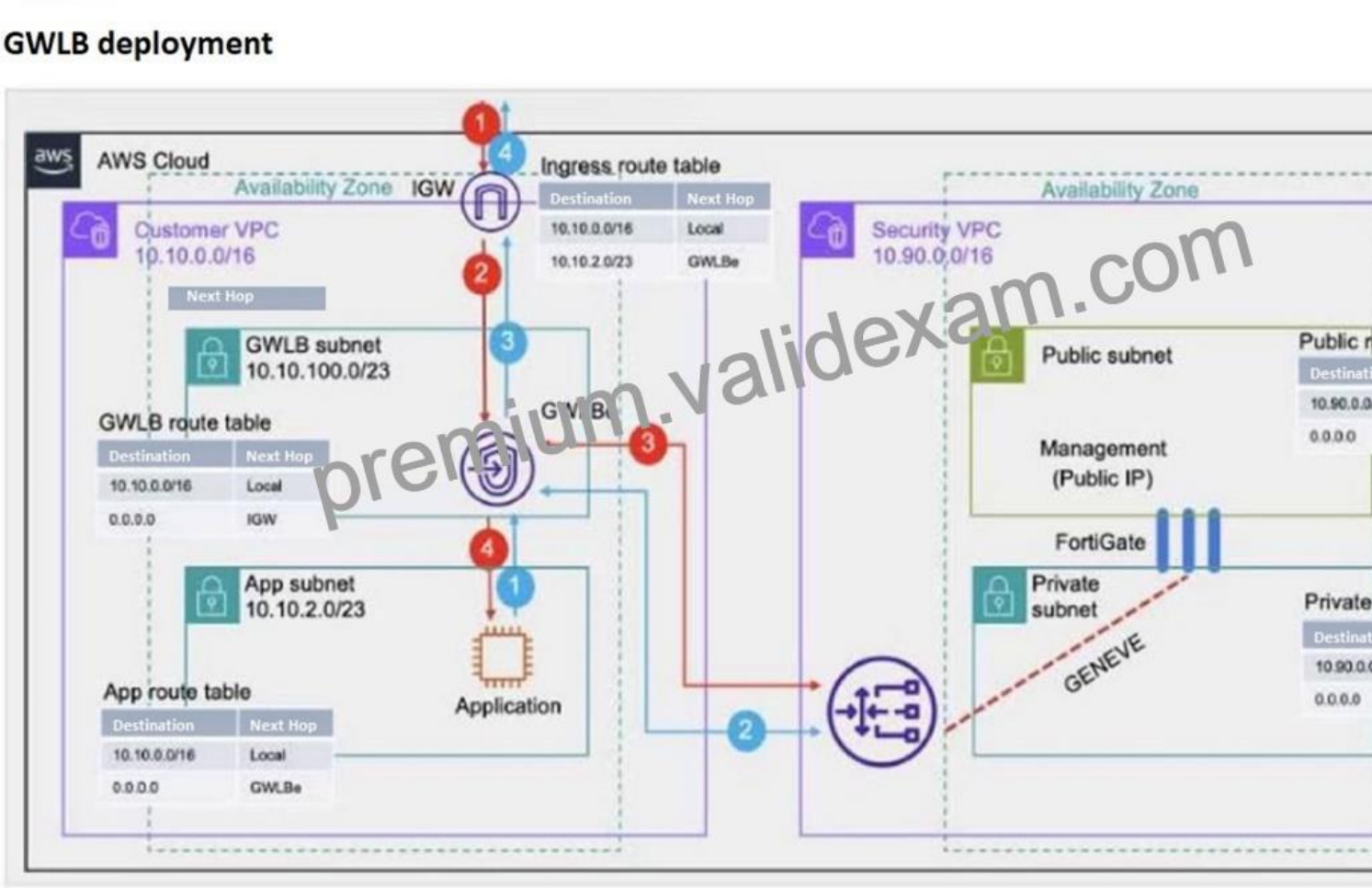
Reference:

AWS Elastic IP Documentation: Elastic IP

AWS Internet Gateway: Internet Gateway

QUESTION 26

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

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).

Other Options Analysis:

Option A is incorrect because GWLB does not forward traffic without encapsulation in its dedicated subnet.

Option C is incorrect as the inbound traffic is directed to the GWLB endpoint first, not directly to the application subnet.

Reference:

AWS Gateway Load Balancer Documentation: AWS GWLB

GENEVE Protocol Overview: GENEVE Protocol

QUESTION 27

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

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.

Reference:

AWS ENI Documentation: Elastic Network Interfaces

AWS Networking Best Practices: AWS Networking

QUESTION 28

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?
* AWS Firewall Manager
* AWS network access control list
* SDN Connector for AWS
* AWS GuardDuty

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.

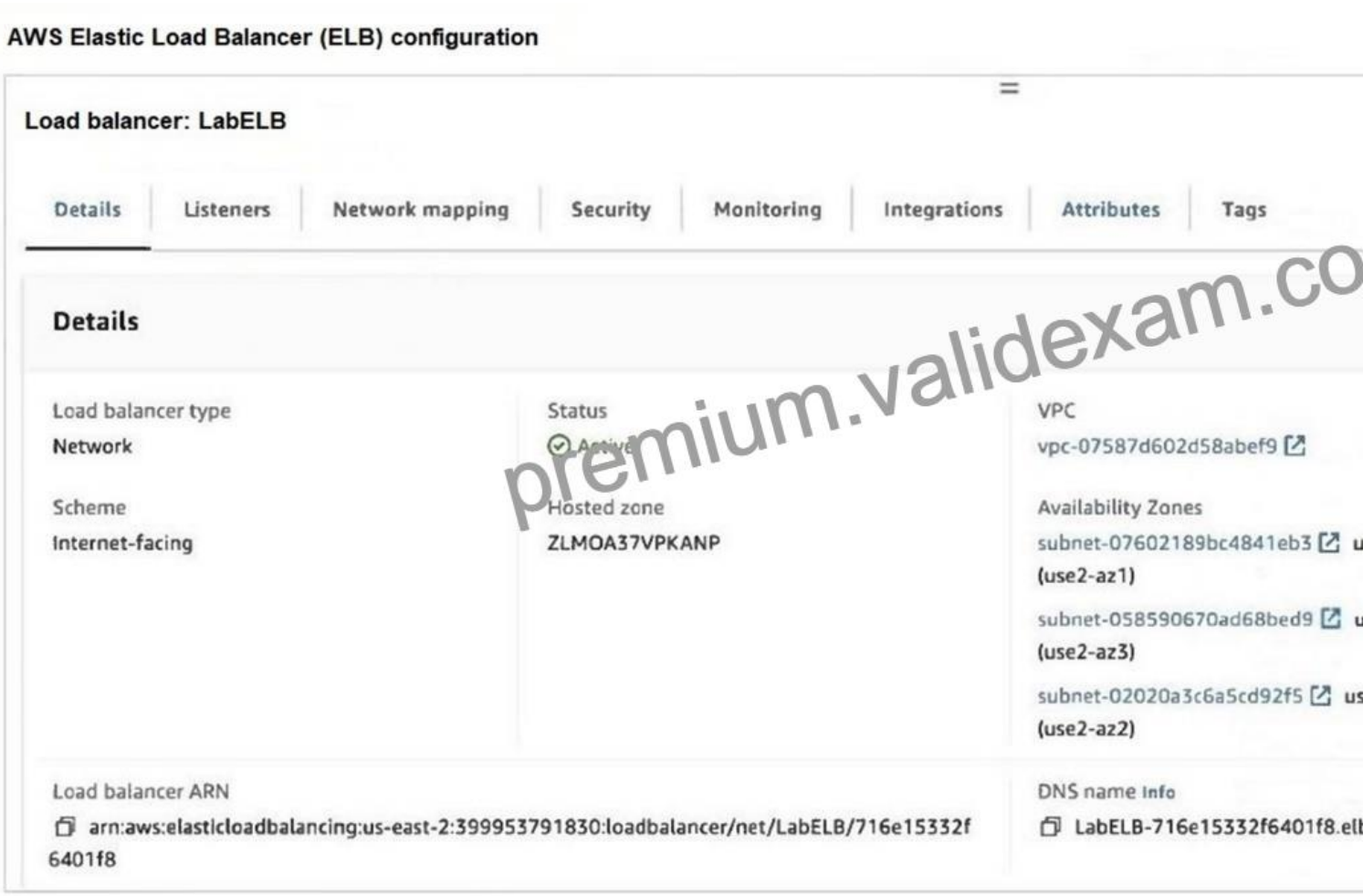
Reference:

AWS GuardDuty: AWS GuardDuty

FortiGate Integration: Fortinet Integration

QUESTION 29

Refer to the exhibit.



A customer is using the AWS Elastic Load Balancer (ELB).

Which two statements are correct about the ELB configuration? (Choose two.)
* The load balancer is configured to load balance traffic among multiple availability zones.
* The Amazon Resource Name is used to access the load balancer node and targets.
* You can use the DNS name to reach the targets behind the ELB.
* The load balancer is configured for the internal traffic of the virtual public cloud (VPC).

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.

Reference:

AWS Elastic Load Balancer Documentation: AWS ELB

Understanding ELB DNS: AWS ELB DNS

QUESTION 30

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.)
* Deploy FortiWeb Cloud in the same region where your web application is being hosted.
* Enable a content delivery network
* Modify DNS entries to directly point to your web server.
* Disable WAF functionality.

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.

Reference:

AWS Regions and Availability Zones: AWS Regions

Content Delivery Network Overview: AWS CloudFront

QUESTION 31

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

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.

Reference:

FortiGate HA in AWS Documentation: FortiGate HA

Fortinet FGCP Details: FGCP Documentation