Number: NSE6_WCS-7.0
Passing Score: 800
Time Limit: 120
File Version: 3.0

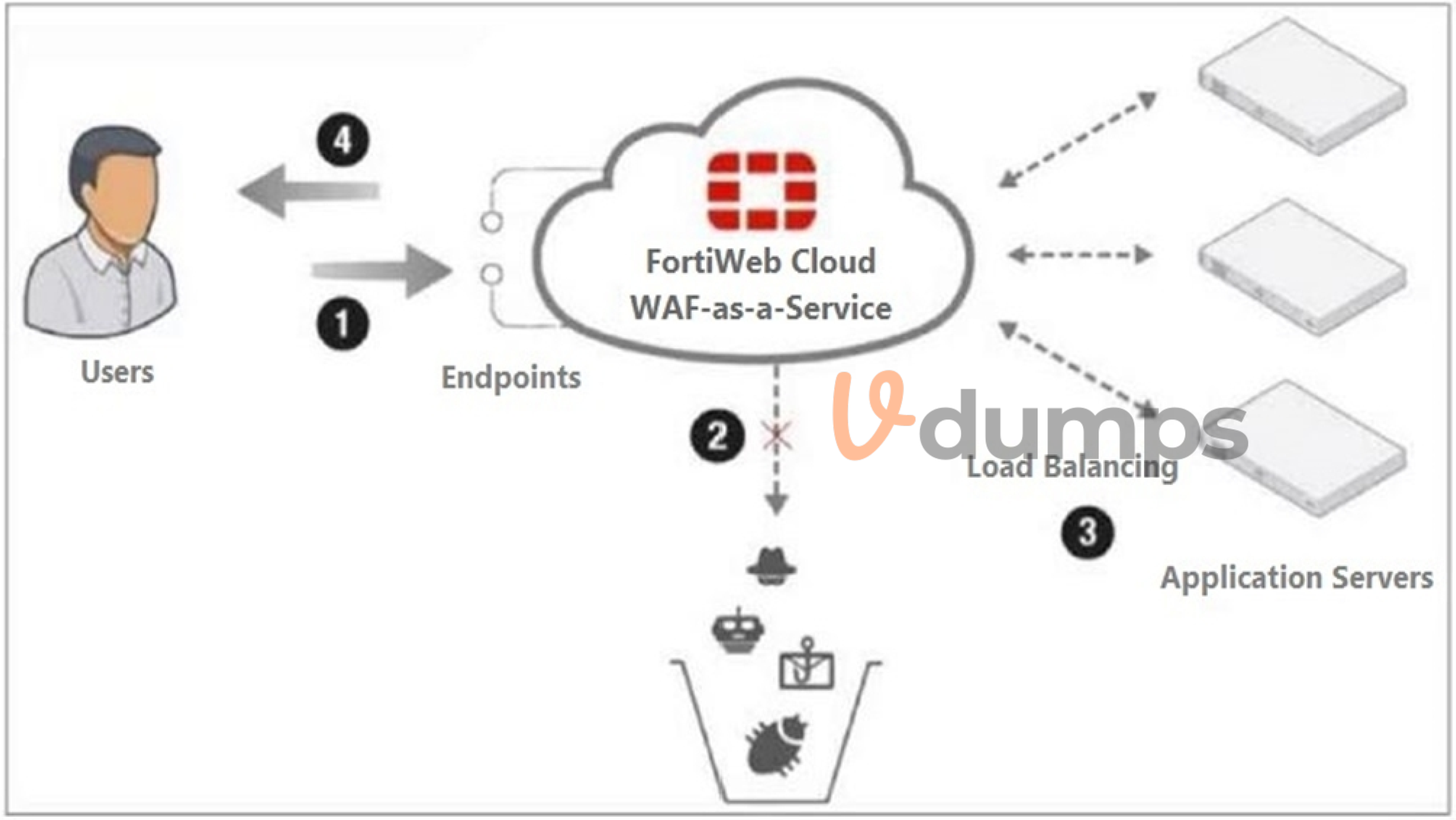
Exam Code: NSE6_WCS-7.0

Exam Name: Fortinet NSE 6 - Cloud Security 7.0 for AWS

Exam A

QUESTION 1
Refer to the exhibit.

FortiWeb Cloud



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 2
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 3
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.)

A. Inbound and outbound traffic will go to multiple devices, which will perform load balancing.
B. Inbound and outbound traffic will go to the same device, which will perform stateful processing.
C. The content of the original traffic exchanged between the GWLB and FortiGate will be preserved.
D. The original traffic exchanged between the GWLB and FortiGate will be hashed for data integrity.

Correct Answer: A, B
Section:
Explanation:
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:

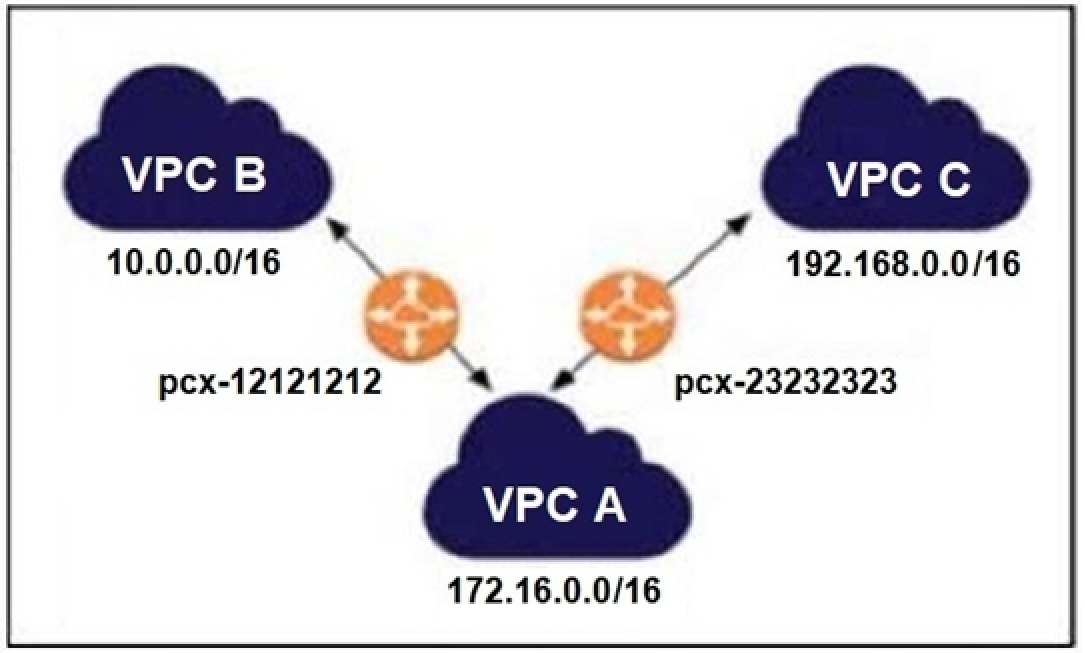
GWLB can send traffic to multiple FortiGate appliances for load balancing purposes, ensuring efficient use of resources (Option A).
Stateful Processing:
For stateful processing, GWLB ensures that traffic flows (both inbound and outbound) for a given connection are directed to the same FortiGate appliance. 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.
AWS Gateway Load Balancer Documentation: AWS Gateway Load Balancer
FortiGate Integration with GWLB: Fortinet Documentation

QUESTION 4
Your organization is deciding between deploying an active-active (A-A) or active-passive (A-P) FortiGate high availability (HA) cluster in AWS cloud.
Which two statements are true about A-A clusters compared to A-P clusters? (Choose two.)

A. For A-A clusters, FortiGate must perform SNAT inbound to ensure symmetric traffic flow.
B. A-A clusters rely on API calls for sfailovers.
C. A-A clusters always require a load balancer.
D. A-A clusters can use a software-defined network (SDN) to perform a failover.

Correct Answer: A, C
Section:
Explanation:
Symmetric Traffic Flow with SNAT:
In active-active (A-A) clusters, symmetric traffic flow is essential for maintaining session integrity across multiple instances. Source Network Address Translation (SNAT) is performed inbound to ensure that return traffic is routed correctly (Option A).
Load Balancer Requirement:
A-A clusters require a load balancer to distribute incoming traffic evenly across the active instances. This is crucial for balancing the load and providing high availability (Option C).
API Calls and Failovers:
Option B is incorrect because failovers in A-A clusters do not typically rely on API calls but are managed by the load balancer and the clustering mechanism itself.
Software-Defined Network (SDN) Failover:
Option D is incorrect as SDN is not specifically required for performing failovers in A-A clusters. The failover mechanism is typically managed by the load balancer and FortiGate's clustering technology.
FortiGate High Availability on AWS: FortiGate HA
AWS Elastic Load Balancing: AWS ELB

QUESTION 5
Refer to the exhibit.

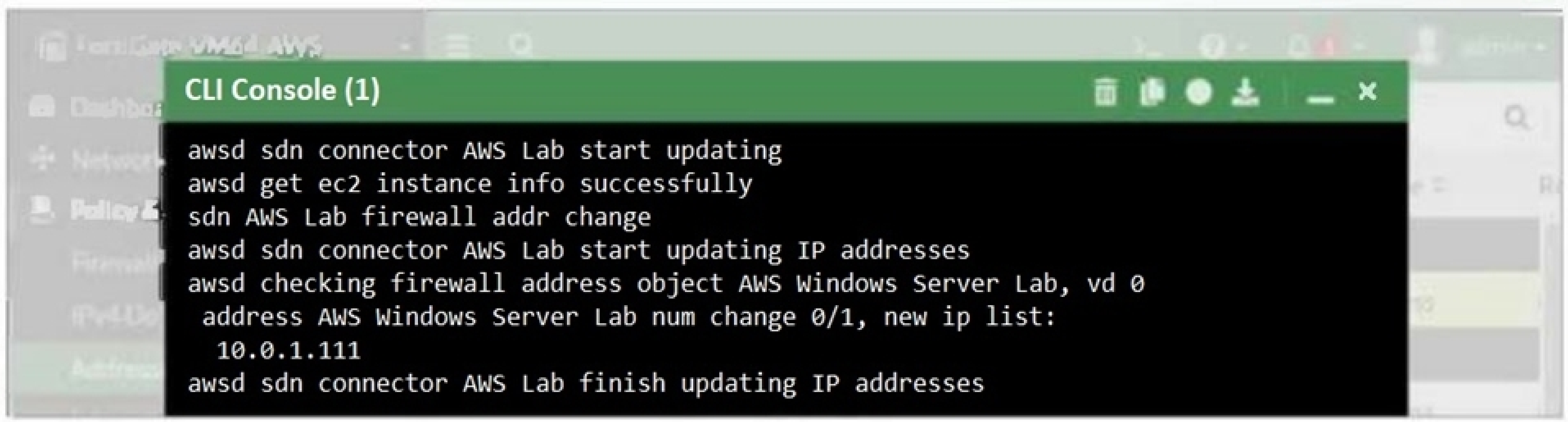


Which statement is correct about the VPC peering connections shown in the exhibit?

A. 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.
B. You cannot route packets directly from VPC B to VPC C through VPC A.
C. You can associate VPC ID pcx-23232323 with VPC B to form a VPC peering connection between VPC B and VPC C.
D. You cannot create a separate VPC peering connection between VPC B and VPC C to route packets directly.

Correct Answer: B
Section:
Explanation:
Understanding VPC Peering:
VPC peering connections allow instances in one VPC to communicate with instances in another VPC. Peering is a one-to-one relationship between two VPCs.
Transit Routing Limitation:
AWS VPC peering connections do not support transitive peering. This means that a packet originating in VPC B cannot be routed through VPC A to reach VPC C. Each pair of VPCs must have its own peering connection.
Routing Table Configuration:
Even if you add a route in the VPC A routing table for the 192.168.0.0/16 network, it won't allow VPC B to communicate with VPC C because of the non-transitive nature of VPC peering.
Comparison with Other Options:
Option A is incorrect because adding a route in VPC A does not overcome the limitation of non-transitive peering.
Option C is incorrect because associating pcx-23232323 with VPC B is not how VPC peering works.
Option D is incorrect because you can create a separate peering connection between VPC B and VPC C, which is the required approach for communication between these VPCs.
AWS VPC Peering Guide: VPC Peering
Limitations of VPC Peering: AWS VPC Peering Limitations

QUESTION 6
Refer to the exhibit.



```
awsd sdn connector AWS Lab start updating
awsd get ec2 instance info successfully
sdn AWS Lab firewall addr change
awsd sdn connector AWS Lab start updating IP addresses
awsd checking firewall address object AWS Windows Server Lab, vd 0
 address AWS Windows Server Lab num change 0/1, new ip list:
  10.0.1.111
awsd sdn connector AWS Lab finish updating IP addresses
```

What two conclusions can you draw from the FortiGate debug output? (Choose two.)

A. The dynamic address object is automatically updated if the IP changes.
B. The address object AWS Windows Server Lab can be manually changed on FortiGate.
C. The SDN connector is correctly configured and authorized.
D. The AWS user account used for software-defined network (SDN) integration must have full administrative rights.

Correct Answer: A, C
Section:
Explanation:
Dynamic Address Object Update:
The debug output shows that the IP address of the AWS Windows Server Lab has been updated automatically, indicating that the dynamic address object feature is working as intended. This allows FortiGate to adapt to changes in the IP addresses of AWS instances dynamically (Option A).
SDN Connector Configuration:
The messages in the debug output confirm that the SDN connector is able to retrieve instance information and update the firewall address objects successfully. This implies that the SDN connector is correctly configured and has the necessary permissions (Option C).
Manual Change and Permissions:
Option B is incorrect because while the address object could theoretically be changed manually, this is not inferred from the debug output.
Option D is incorrect because the debug output does not indicate that the AWS user account must have full administrative rights. The required permissions are typically more scoped to specific actions related to SDN.
FortiGate AWS Integration Guide: FortiGate on AWS
AWS IAM Policies for SDN: AWS IAM Policies

QUESTION 7
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 8
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 9
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

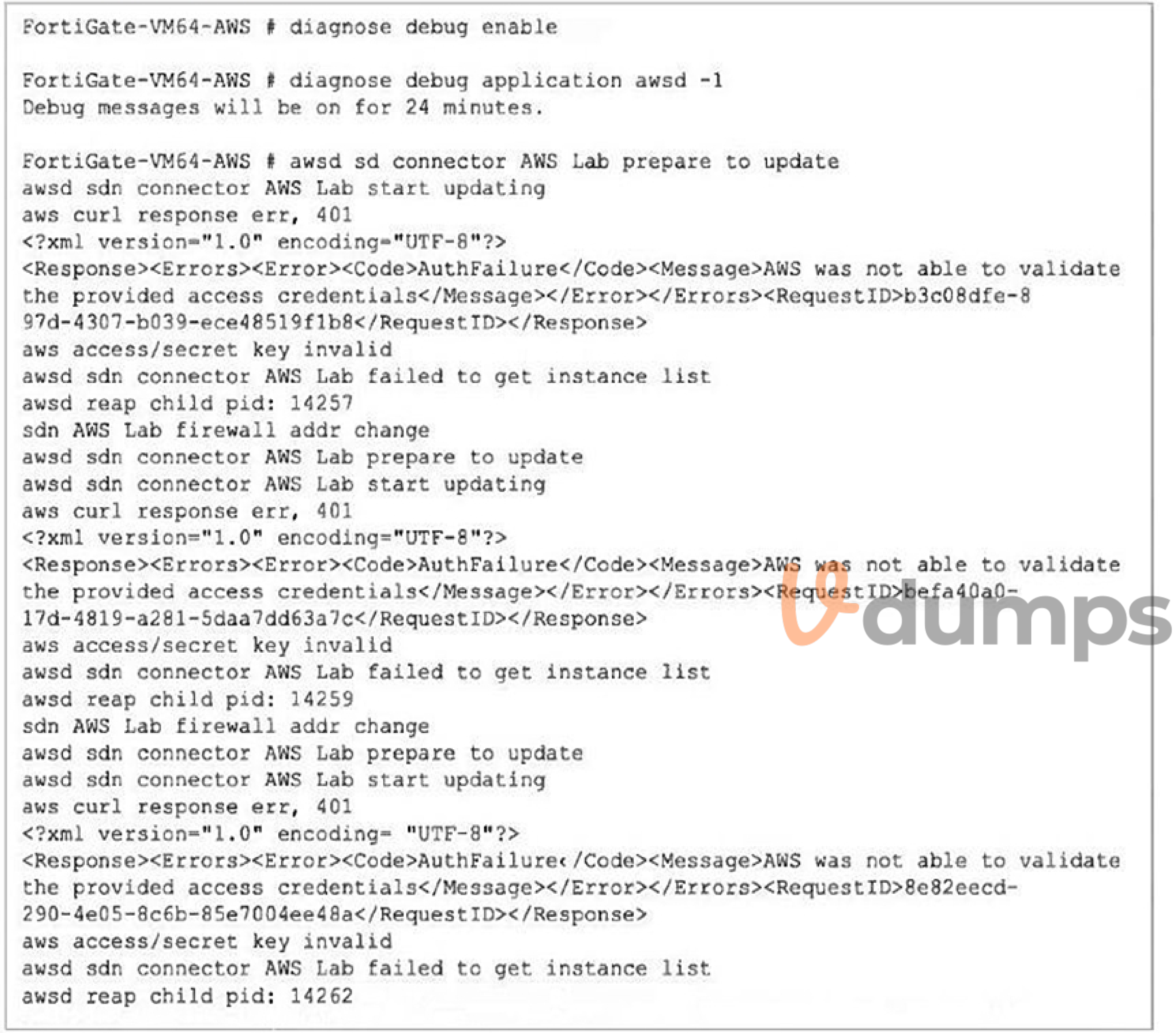
Correct Answer: C, D, E
Section:
Explanation:

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 10

Refer to the exhibit.

FortiGate debug output



```
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 sd 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
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>befa40a0-
17d-4819-a281-5daa7dd63a7c</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14259
sdn AWS Lab firewall addr change
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>8e82eecd-
290-4e05-8c6b-85e7004ee48a</RequestID></Response>
aws access/secret key invalid
awsd sdn connector AWS Lab failed to get instance list
awsd reap child pid: 14262
```

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

Which two reasons can explain why? (Choose two.)

A. The AWS API call is not supported on XML version 1.0.

B. AWS was not able to validate credentials provided by the AWS Lab SDN connector because of a clock skew between FortiGate and AWS.

C. The AWS Lab SDN connector is configured with an invalid AWS access or secret key.

D. The AWS Lab SDN connector failed to connect on port 401.

E. The AWS Lab SDN did not find any instances in the configured VPC.

Correct Answer: B, C
Section:
Explanation:
Invalid Credentials:
The debug output shows an 'AuthFailure' error, indicating that AWS was not able to validate the provided access credentials. This usually points to incorrect or invalid AWS access or secret keys configured in the AWS Lab SDN connector (Option C).
Clock Skew:
Another common reason for authentication failures in AWS API calls is a clock skew between the FortiGate device and AWS. AWS requires that the system time of the client making the API call is synchronized with its own time, within a small margin. If there is a significant time difference, AWS will reject the credentials (Option B).
Other Options Analysis:
Option A is incorrect because the AWS API supports XML version 1.0.
Option D is incorrect as the error message does not indicate an issue with connecting on port 401.
Option E is incorrect because the error is related to authentication, not the absence of instances.
AWS API Authentication: AWS API Security
FortiGate AWS Integration Guide: FortiGate AWS Integration

QUESTION 11
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 12
A customer has deployed FortiGate Cloud-Native Firewall (CNF).
Which two statements are correct about policy sets? (Choose two.)

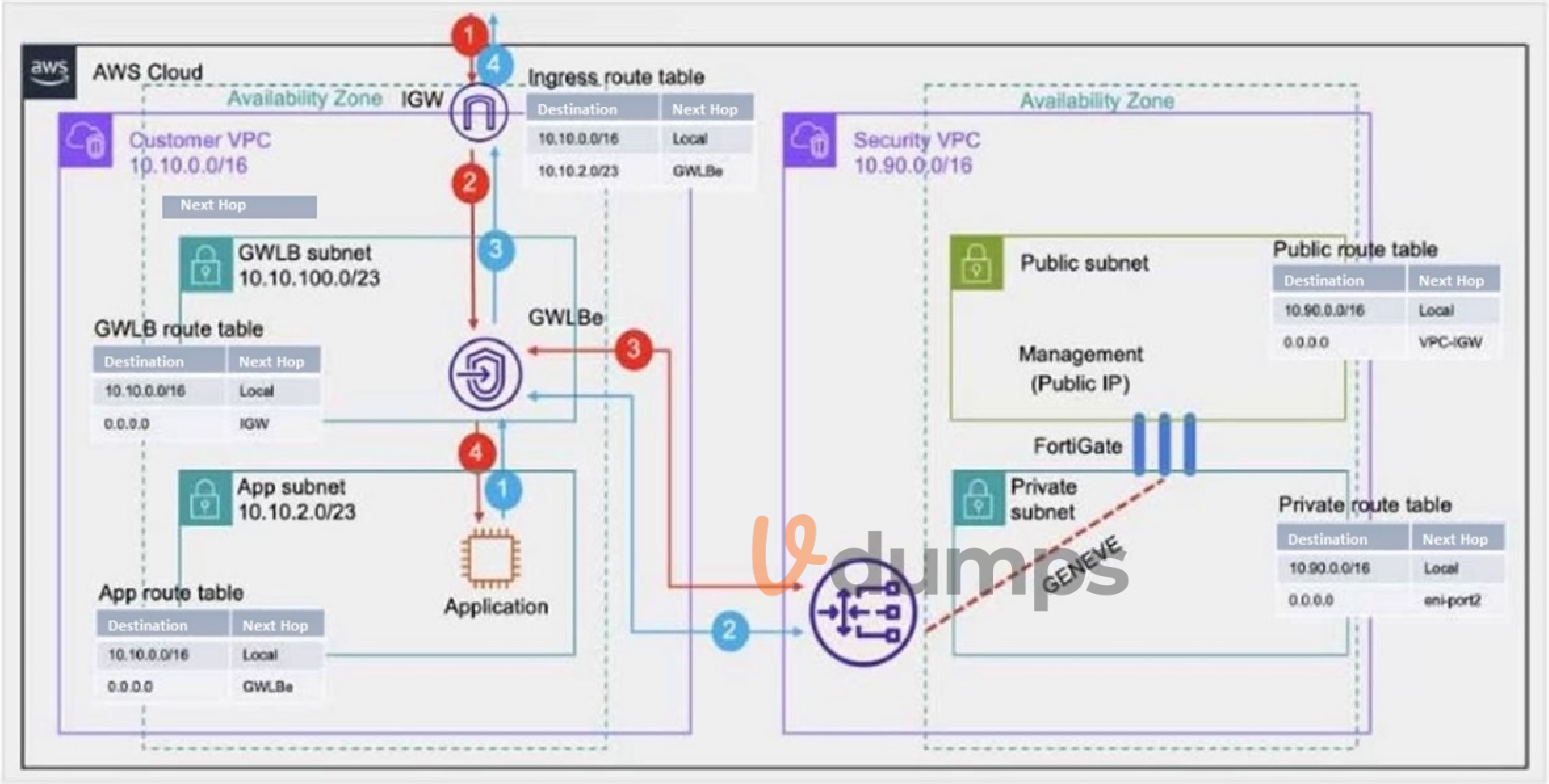
A. There is an implicit deny rule at the bottom of the policy set.
B. The policy set must be manually synchronized to the CNF instance each time it is modified.
C. A new policy set is created with each deployed CNF instance.

D. Multiple policy sets can be applied to a single CNF instance.

Correct Answer: A, C
Section:
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).
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.
FortiGate CNF Documentation: FortiGate CNF
Firewall Policy Best Practices: Fortinet Policies

QUESTION 13
Refer to the exhibit.

GWLB deployment



Ingress route table

Destination	Next Hop
10.10.0.0/16	Local
10.10.2.0/23	GWLBe

GWLB route table

Destination	Next Hop
10.10.0.0/16	Local
0.0.0.0	IGW

App route table

Destination	Next Hop
10.10.0.0/16	Local
0.0.0.0	GWLBe

Public route table

Destination	Next Hop
10.90.0.0/16	Local
0.0.0.0	VPC-IGW

Private route table

Destination	Next Hop
10.90.0.0/16	Local
0.0.0.0	eni-port2

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

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.

Correct Answer: B, D
Section:
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).

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.
AWS Gateway Load Balancer Documentation: AWS GWLB
GENEVE Protocol Overview: GENEVE Protocol

QUESTION 14
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.

Correct Answer: A, D
Section:
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).
Other Options Analysis:
Option B is incorrect because the default AWS Network Access Control List (NACL) allows all inbound and outbound traffic.
Option C is incorrect as AWS does allow ICMP traffic between subnets if properly configured with Security Groups and NACLs.
AWS Security Groups: AWS Security Groups
Windows Firewall Configuration: Windows Firewall

QUESTION 15
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 16
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 17
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 18
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 19
A global organization with cloud networks deployed in several AWS regions wants to set up next-generation firewall (NGFW) protection using FortiGate Cloud-Native Firewall (CNF).
What are two deployment considerations for the organization? (Choose two.)

A. They must choose AWS Firewall Manager to provision a CNF instance.
B. A CNF instance is required for each AWS region that must be protected.
C. More than one AWS account can be associated with a CNF instance.
D. Only one CNF instance is required to protect all AWS regions.

Correct Answer: B, C
Section:
Explanation:
Regional Deployment:
For a global organization with cloud networks in multiple AWS regions, a separate FortiGate Cloud-Native Firewall (CNF) instance is required for each AWS region to provide localized protection and meet compliance requirements. This ensures that each region has its own dedicated NGFW protection tailored to its specific needs (Option B).
Multi-Account Association:
FortiGate CNF supports associating multiple AWS accounts with a single CNF instance. This feature is beneficial for organizations that operate in a multi-account setup, allowing centralized management and security policies

across different accounts (Option C).
Other Options Analysis:
Option A is incorrect because AWS Firewall Manager is a different service and is not required to provision a CNF instance.
Option D is incorrect because a single CNF instance cannot protect multiple AWS regions due to regional isolation in AWS.
FortiGate CNF Documentation: FortiGate CNF
AWS Multi-Account Best Practices: AWS Multi-Account

QUESTION 20
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?

A. Create and associate a public subnet with the primary ENI of the FortiGate VM, and then assign the EIP to the primary ENI.
B. Shut down the FortiGate VM, if it is running, assign the EIP to the primary ENI, and then power it on.
C. Create and attach an internet gateway to the VPC, and then assign the EIP to the primary ENI of the FortiGate VM.
D. 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.

Correct Answer: C
Section:
Explanation:
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.
AWS Elastic IP Documentation: Elastic IP
AWS Internet Gateway: Internet Gateway