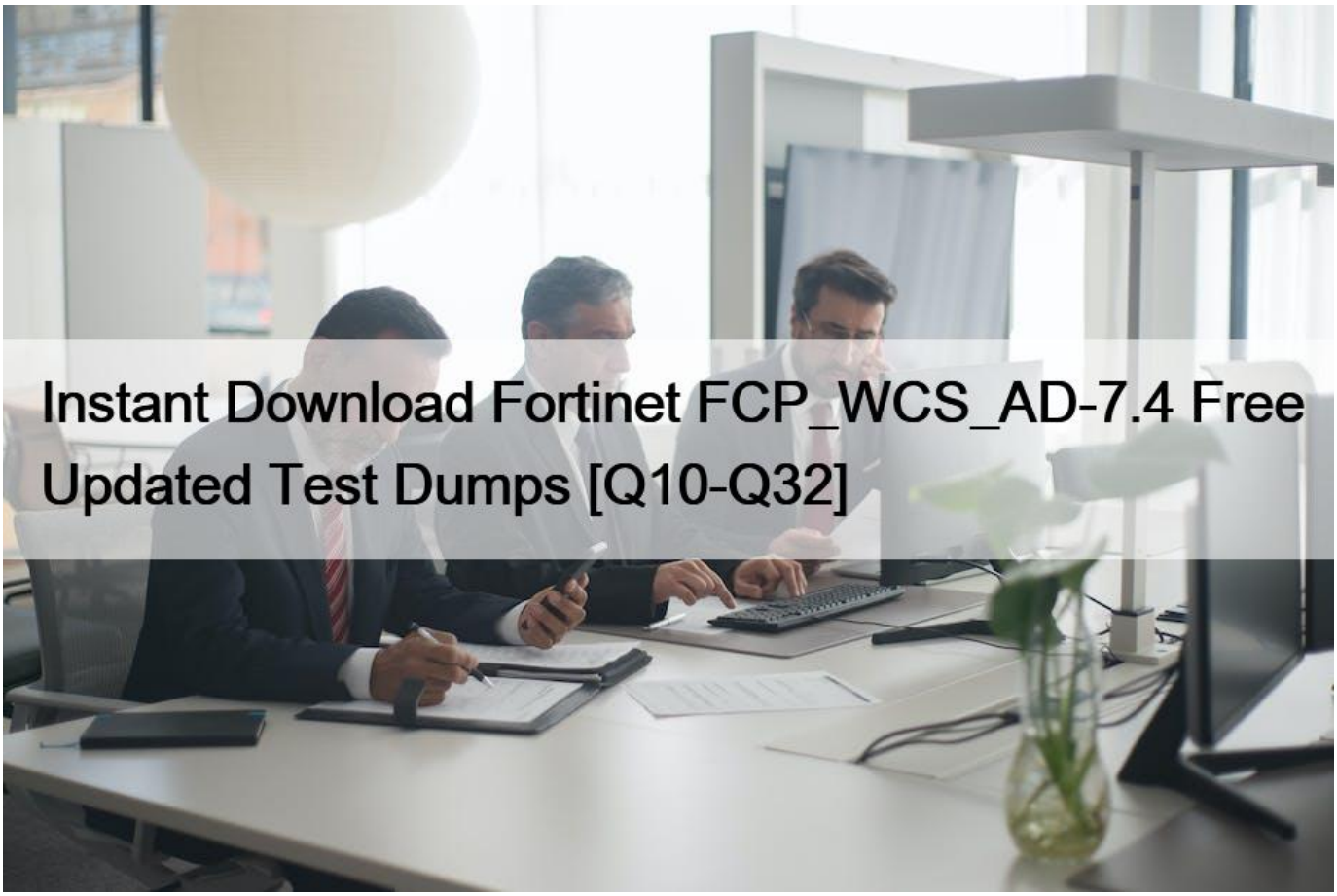
Instant Download Fortinet FCP_WCS_AD-7.4 Free Updated Test Dumps [Q10-Q32



Instant Download Fortinet: FCP_WCS_AD-7.4 Free Updated Test Dumps
Valid FCP_WCS_AD-7.4 FREE EXAM DUMPS QUESTIONS & ANSWERS

NEW 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>b3c08df1-8
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.)
* The AWS API call is not supported on XML version 1.0.
* AWS was not able to validate credentials provided by the AWS Lab SDN connector because of a clock skew between FortiGate and AWS.
* The AWS Lab SDN connector is configured with an invalid AWS access or secret key.
* The AWS Lab SDN connector failed to connect on port 401.
* The AWS Lab SDN did not find any instances in the configured VPC.

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.

Reference:

AWS API Authentication: AWS API Security

FortiGate AWS Integration Guide: FortiGate AWS Integration

NEW QUESTION 11

AWS native network services offer vast functionality and inter-connectivity between the cloud and on-premises networks.

Which three additional functions can FortiGate for AWS offer to complement the native services offered by AWS? (Choose three.)
* Higher VPN throughput
* Web filtering
* OSPF over IPSec
* Advanced dynamic routing
* Secure SD-WAN with application visibility

Web Filtering:

FortiGate for AWS offers advanced web filtering capabilities, which allow organizations to control and monitor web access. This feature complements AWS’s native security services by providing granular control over web traffic (Option B).

OSPF over IPSec:

FortiGate for AWS can establish dynamic routing protocols such as OSPF (Open Shortest Path First) over IPSec tunnels. This capability enhances network routing flexibility and security, which is not natively provided by AWS (Option C).

Secure SD-WAN with Application Visibility:

FortiGate for AWS provides Secure SD-WAN functionality, offering enhanced application visibility and traffic management. This is a significant addition to AWS’s networking services, optimizing application performance and security (Option E).

Comparison with Other Options:

Option A (Higher VPN throughput) is not specifically enhanced by FortiGate as compared to AWS native services.

Option D (Advanced dynamic routing) is partially covered under OSPF over IPSec but is not as specific as the other chosen options.

Reference:

FortiGate for AWS Documentation: FortiGate on AWS

AWS Networking and Content Delivery: AWS Networking

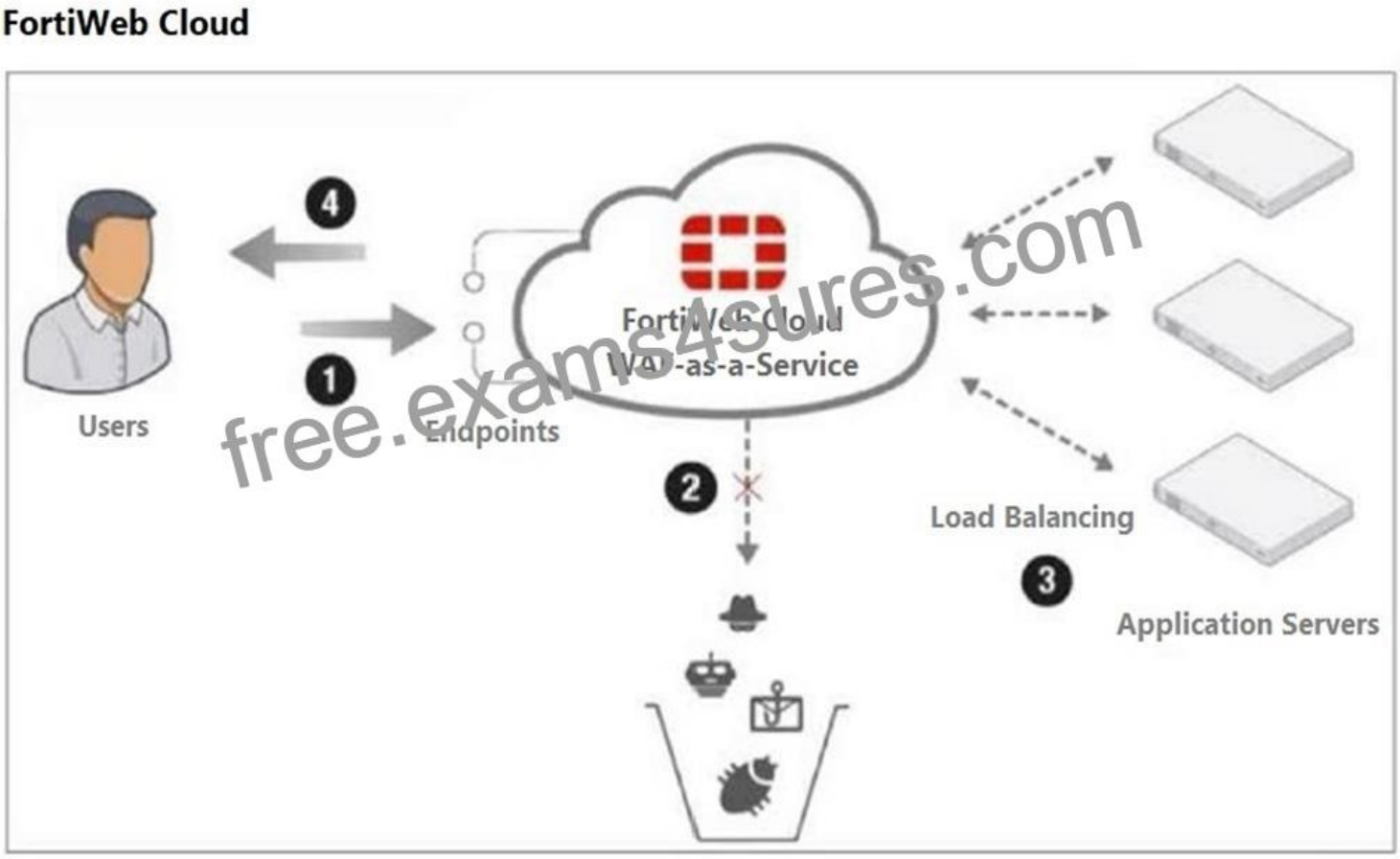
NEW QUESTION 12

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

NEW QUESTION 13

Refer to the exhibit.



Which two statements are correct about traffic flow in FortiWeb Cloud? (Choose two.)
* The DNS name for the application servers must point to FortiWeb Cloud.
* FortiWeb Cloud filters the incoming traffic from users, blocking the OWASP Top 10 attacks, zero-day threats, and other application layer attacks.
* FortiWeb Cloud can protect the application servers only if they are all located in the same virtual public cloud (VPC).
* Step 2 requires an AWS S3 bucket to be created.
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.

Reference:

FortiWeb Cloud Overview: FortiWeb Cloud

DNS Configuration for Web Applications: DNS Configuration

NEW QUESTION 14

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

NEW QUESTION 15

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

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.

Reference:

FortiGate CNF Documentation: FortiGate CNF

AWS Multi-Account Best Practices: AWS Multi-Account

NEW QUESTION 16

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

NEW QUESTION 17

Your company deployed a FortiSandbox for AWS.

Which statement is correct about FortiSandbox for AWS?
* 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.
* The FortiSandbox manager is installed on the AWS platform and analyzes the results of the sandboxing process received from on-premises Windows instances.
* FortiSandbox for AWS does not need more resources because it performs only management and analysis tasks.
* FortiSandbox deploys new EC2 instances with the custom Windows and Linux VMs, then it sends malware, runs it, and captures the results for analysis.
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.

Reference:

FortiSandbox for AWS Documentation: FortiSandbox

Sandboxing Concepts: Sandboxing

NEW QUESTION 18

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

NEW QUESTION 19

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

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.

Reference:

AWS Shared Responsibility Model: AWS Shared Responsibility

EC2 Security Best Practices: AWS EC2 Security

NEW QUESTION 20

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

NEW QUESTION 21

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 elas
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?
* The routing table for Fgt2 updated successfully, and port2 will provide internet access to Fgt2.
* The Elastic IP is associated with port1 of Fgt2.
* IP address 10.0.0.13 is now associated with eni-0b61d8afc0aefb8a2.
* The Elastic IP is associated with port2 of Fgt2, and the secondary IP address for port1 and port2 was updated successfully.

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.

Reference:

FortiGate HA Configuration Guide: FortiGate HA

AWS Elastic IP Documentation: Elastic IP

NEW QUESTION 22

An administrator has been asked to deploy an active-passive (A-P) FortiGate cluster in the AWS cloud across two availability zones.

In addition to enhanced redundancy, which other major difference is there compared to deploying A-P high availability in the same availability zone?
* The FortiGate devices act as a single, logical instance.
* Secondary IP address configuration is used.
* The number of subnets required is less.
* IP addressing and subnetting are not shared.

Enhanced Redundancy:

Deploying an active-passive (A-P) FortiGate cluster across two availability zones (AZs) provides enhanced redundancy by ensuring that if one AZ fails, the other can take over, maintaining high availability and uptime.

IP Addressing and Subnetting:

One of the major differences when deploying across different AZs compared to the same AZ is that IP addressing and subnetting are not shared between the instances. Each AZ operates independently with its own set of subnets and IP addresses, which must be managed separately (Option D).

Other Options Analysis:

Option A is incorrect because the FortiGate devices in an A-P setup do not act as a single logical instance; they operate in a failover setup.

Option B is incorrect because secondary IP address configuration is used in both single AZ and multi-AZ deployments.

Option C is incorrect because the number of subnets required is typically more when deploying across multiple AZs for redundancy.

Reference:

FortiGate HA Configuration Guide: FortiGate HA

AWS Availability Zones: AWS AZ

NEW QUESTION 23

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

NEW QUESTION 24

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.)
* AWS WAF
* FortiEDR
* FortiGate Cloud-Native Firewall (CNF)
* Fortinet Managed Rules for AWS WAF
* FortiWeb Cloud

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.

Reference:

FortiGate CNF Documentation: FortiGate CNF

Fortinet Managed Rules for AWS WAF: Fortinet AWS WAF Rules

FortiWeb Cloud Overview: FortiWeb Cloud

Fortinet FCP_WCS_AD-7.4 Exam Syllabus Topics:

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

Free FCP_WCS_AD-7.4 Exam Braindumps Fortinet Pratice Exam:
https://www.exams4sures.com/Fortinet/FCP_WCS_AD-7.4-practice-exam-dumps.html]